PERFORMANCE AND SECURITY TRADE-OFFS IN HIGH-SPEED NETWORKS

G. M. A. MISKEEN

PhD

UNIVERSITY OF BRADFORD

2013

Performance and Security Trade-offs in High-Speed Networks

An investigation into the performance and security modelling and evaluation of high-speed networks based on the quantitative analysis and experimentation of queueing networks and generalised stochastic Petri nets

Guzlan Mohamed Alzaroug MISKEEN

Submitted for the degree of

Doctor of Philosophy

Department of Computing

School of Computing, Informatics and Media

University of Bradford

2013

Keywords: Performance, security, high-speed network, queueing network, generalised stochastic Petri net.

Abstract

Most used security mechanisms in high-speed networks have been adopted without adequate quantification of their impact on performance degradation. Appropriate quantitative network models may be employed for the evaluation and prediction of 'optimal' performance vs. security trade-offs. Several quantitative models introduced in the literature are based on queueing networks (QNs) and generalised stochastic Petri nets (GSPNs). However, these models do not take into consideration Performance Engineering Principles (PEPs) and the adverse impact of traffic burstiness and security protocols on performance.

The contributions of this thesis are based on the development of an effective quantitative methodology for the analysis of arbitrary QN models and GSPNs through discrete-event simulation (DES) and extended applications into performance vs. security trade-offs involving infrastructure and infrastructure-less high-speed networks under bursty traffic conditions. Specifically, investigations are carried out focusing, for illustration purposes, on high-speed network routers subject to Access Control List (ACL) and also Robotic Ad Hoc Networks (RANETs) with Wired Equivalent Privacy (WEP) and Selective Security (SS) protocols, respectively. The Generalised Exponential (GE) distribution is used to model inter-arrival and service times at each node in order to capture the traffic burstiness of the network and predict pessimistic 'upper bounds' of network performance.

In the context of a router with ACL mechanism representing an infrastructure network node, performance degradation is caused due to high-speed incoming traffic in conjunction with ACL security computations making the router a bottleneck in the network. To quantify and predict the trade-off of this degradation, the proposed quantitative methodology employs a suitable QN model consisting of two queues connected in a tandem configuration. These queues have single or quad-core CPUs with multiple-classes and correspond to a security processing node and a transmission forwarding node. First-Come-First-Served (FCFS) and Head-of-the-Line (HoL) are the adopted service disciplines together with Complete Buffer Sharing (CBS) and Partial Buffer Sharing (PBS) buffer management schemes. The mean response time and packet loss probability at each queue are employed as typical performance metrics. Numerical experiments are carried out, based on DES, in order to establish a balanced trade-off between security and performance towards the design and development of efficient router architectures under bursty traffic conditions.

The proposed methodology is also applied into the evaluation of performance vs. security trade-offs of robotic ad hoc networks (RANETs) with mobility subject to Wired Equivalent Privacy (WEP) and Selective Security (SS) protocols. WEP protocol is engaged to provide confidentiality and integrity to exchanged data amongst robotic nodes of a RANET and thus, to prevent data capturing by unauthorised users. WEP security mechanisms in RANETs, as infrastructure-less networks, are performed at each individual robotic node subject to traffic burstiness as well as nodal mobility. In

this context, the proposed quantitative methodology is extended to incorporate an open QN model of a RANET with Gated queues (G-Queues), arbitrary topology and multiple classes of data packets with FCFS and HoL disciplines under bursty arrival traffic flows characterised by an Interrupted Compound Poisson Process (ICPP). SS is included in the Gated-QN (G-QN) model in order to establish an 'optimal' performance vs. security trade-off. For this purpose, PEPs, such as the provision of multiple classes with HoL priorities and the availability of dual CPUs, are complemented by the inclusion of robot's mobility, enabling realistic decisions in mitigating the performance of mobile robotic nodes in the presence of security. The mean marginal end-to-end delay was adopted as the performance metric that gives indication on the security improvement.

The proposed quantitative methodology is further enhanced by formulating an advanced hybrid framework for capturing 'optimal' performance vs. security trade-offs for each node of a RANET by taking more explicitly into consideration security control and battery life. Specifically, each robotic node is represented by a hybrid Gated GSPN (G-GSPN) and a QN model. In this context, the G-GSPN incorporates bursty multiple class traffic flows, nodal mobility, security processing and control whilst the QN model has, generally, an arbitrary configuration with finite capacity channel queues reflecting 'intra'-robot (component-to-component) communication and 'inter'-robot transmissions. Two theoretical case studies from the literature are adapted to illustrate the utility of the QN towards modelling 'intra' and 'inter' robot communications. Extensions of the combined performance and security metrics (CPSMs) proposed in the literature are suggested to facilitate investigating and optimising RANET's performance vs. security trade-offs.

This framework has a promising potential modelling more meaningfully and explicitly the behaviour of security processing and control mechanisms as well as capturing the robot's heterogeneity (in terms of the robot architecture and application/task context) in the near future (c.f. [1]. Moreover, this framework should enable testing robot's configurations during design and development stages of RANETs as well as modifying and tuning existing configurations of RANETs towards enhanced 'optimal' performance and security trade-offs.

Declaration

I hereby declare that this thesis has been genuinely carried out by myself and has not been used in any previous application for a degree. Chapters 5 to 7 describe work performed in conjunction with my supervisor, Prof. D. D. Kouvatsos. These chapters have been accepted for publication (as shown in the publication list). The invaluable participation of others in this thesis has been acknowledged where appropriate.

Guzlan Mohamed Alzaroug Miskeen

Dedication

This thesis is dedicated to my beloved parents, whose love, help, support and prayers are the reason why I am where I am today, and my beloved sisters and brothers, in particular Sakina, Hashem and Musbah. This work is also dedicated to the soul of my uncle, Abo Zaid, whom we lost in the Libyan war in 2011.

Acknowledgements

In the Name of Allah, the Most Gracious, the Most Merciful. All Praise is Due to Allah for His Glorious Ability and Great Power. I would like to thank Allah for giving me the power, patience and knowledge to complete this doctoral thesis.

I would like to express my gratitude to all those who gave me the support and encouragement to complete this thesis. First of all, I would like to express my sincere appreciation and profound gratitude to my supervisor Professor Demetres Kouvatsos, who provided invaluable guidance throughout the course of this research. I would like to express my appreciation for his helpful suggestions, continual and unwavering encouragements, patience, kindness and endless support throughout the entire research and thesis writing process.

I would like to express my appreciation to all the staff at the Department of Computing's technical support office as well as Hub and the library. I would also like to thank my colleagues: Dr. Monis Akhlaq, Mr. Esmaeil Habibzadeh, Mr. Neel Kamal Shah, Dr. Roquia Abdelrahman for their fruitful discussions suggestions an co-operation.

I am deeply indebted to my family, relatives and friends who offered me great support and encouragement throughout my studies. My heartfelt thanks go to my parents, my sisters and my brothers for their unfailing love, prayers continuous support and patience.

Many thanks also go to all of my friends, who support and encourage me, in particular; Mona Masud, Asma Said, Einasse Madani, Mrs. Huda Salem and family, Abeer Hamdu and family, Soad Sahel and family, Mr. Rashid Munir and Mrs Sumira Rashid, Mrs Roquia Musbah and family, Fatima Hothali, Hind Abdulgader, Yasmin Bashon, Antisar Shabut, Fawzia Jaber and Shumaila Ansari. I'd like also to express my thanks to my lecturers: Dr. Mohamad Salem, Dr.Falah Jawad and Dr. Yasser Lamey for their continuous support.

Finally, I would like to gratefully acknowledge the provision of the scholarship from the Ministry of Higher Education in Libya and the Libyan Cultural Attaché bureau in London.

Publications

Workshops

Miskeen, G.M.A, Kouvatsos, D. D., & Akhlaq, M., (2010). Performance and Security Trade-off for Routers in High-Speed Networks. In S. Hammond, S. Jarvis, & M. Leeke (Eds.), UK Performance Engineering Workshop, University of Warwick, 8-9 July 2010, (pp. 119-128).

Miskeen, G. M. A, Kouvatsos, D. D., (2011). Performance Related Security Trade-off for Routers in High-Speed Networks, UK Performance Engineering Workshop, University of Bradford, July 2011.

Journals

Kouvatsos, D. D., and Miskeen, G. M. A., (2012). Performance Related Security Modelling and Evaluation of RANETs. Wireless Personal Communications, 64, 523-546, doi:10.1007/s11277-012-0599-1.

Miskeen G. M. A., Kouvatsos, D. D., and Habibzadeh E., (2013). An Exposition of Performance-Security Trade-offs in RANETs Based on Quantitative Network Models, Wireless Personal Communications, 2013, Vol. 70, Issue 3, June 2013, 1121-1146, DOI 10.1007/s11277-013-1105-0.

Kouvatsos, D. D., Miskeen, G.M.A and Habibzadeh E., (2013). Performance Modelling and Evaluation of Secure Dynamic Group Communication Systems in RANETs, in preparation.

Technical Reports

Miskeen, G. M. A., (2011). A Portfolio of simulation programs in java for the analysis of arbitrary open G-QN Models, Technical Tutorial, TT-07-2011 NetPEn Research Group, (I. R. I). University of Bradford, Bradford, UK).

Miskeen, G. M. A., (2011). On the Simulation of GE, Technical Tutorial, NetPEn Research Group, IRI, University of Bradford, Bradford, UK).

Kouvatsos, D. D., and Miskeen, G. M. A., (2011). Networked mobile wireless robotics, Technical Report, Networks and Performance Engineering (NetPEn) Research Group, (I. R. I.) TR-06-2011 University of Bradford).

Miskeen, G. M. A. and Kouvatsos, D.D., (2011). On the Simulation of the GE-type Distribution, Technical Tutorial TT-06-2011, NetPEn-Networks and Performance Engineering Research Group, Informatics Research Institute (IRI). University of Bradford.

Posters

Miskeen, G. M.A., Kouvatsos, D. D., and Akhlaq, M. Performance Related Security in High Speed Networks., (2010). In London Hopper 2010- Poster Competition in the 4th of May 2010.

Miskeen, G. M. A., Kouvatsos, D. D., (2010), Performance vs. Security for the Routers in High-Speed Networks. In the Exhibition of Libyan Engineers Society in Nottingham 17th of July 2010.

List of Acronyms

ACL	Access Control List
BMAP	Batch Markovian Arrival Process
BRP	Batch Renewal Proces
CBS	Complete Buffer Sharing
CDF	Cumulative Distribution Function
CFPN	Coloured Fuzzy Petri Nets
CPP	Compound Poisson Process
CPSM	Combined Performance and Security Measure
CRAHNs	Cognitive Radio Mobile Wireless Ad Hoc Networks
CRC	Cyclic Redundancy Check
DES	Discrete-Event Simulation
DoS	Denial of Service
FCFS	First-Come-First-Served
GCS	Group Communication System
G-QNs	Gated QNs
G- Queue	Gated-Queue
G-GSPN_QN	Gated-Generalised Stochastic Petri Nets_ QNs
GE	Generalised Exponential
GSPNs	Generalised Stochastic Petri Nets
HoL	Head-of-the-Line
ICPP	Interrupted Compound Poisson Process
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ETSI	European Telecommunications Standards Institute
FPNs	Fuzzy Petri Nets
IDC	Index of Dispersion for Counts
IDI	Index of Dispersion for Intervals
IPP	Interrupted Poisson Process
LAN	Local Area Network
MANETs	Mobile Ad Hoc Networks
MC-PNiQ	Multi Class-Petri Nets including Queuing networks
ME	Maximum Entropy
MMPP	Markov Modulated Poisson Process
MQL	Mean Queue Length

MTTF	Mean Time To Security Failure
OSI	Open Systems Interconnection
PBS	Partial Buffer Sharing
PDF	Probability Density Function
PEPs	Performance Engineering Principles
PNs	Petri Nets
PNiQ	Petri nets including queuing networks
PLP	Packet Loss Probability
PFQN	Product-Form Queueing Networks
RANETs	Robotic Ad Hoc Networks
RS-FD	Repetitive Service-Fixed Destination
RS-RD	Repetitive Service-Random Destination
QNs	Queueing Networks
QoS	Quality-of-Service
SCV	Squared Coefficient of Variation
SPNs	Stochastic Petri Nets
SS	Selective Security
TPNs	Timed Petri Nets
TTPNs	Timed Transitions PNs
WEP	Wired Equivalent Privacy
WPA	Wi Fi Protected Access

List of Contents

List of Tables

List of Figures

Chapter 1 Introduction

1.1 Introduction

High-speed networks have become the backbone of large network installations; therefore, it is vital to design secure networks of greater capacity that support high-volume traffic (c.f., [2 , 3 , 4]). Most security mechanisms embedded within these networks, such as access controls and encryptions, are adopted without any explicit determination of how they will affect the performance due to processing additional bits and performing more computations(c.f., [3 , 5]). Thus there is a great need to trade off between performance and security [6]. By trading off, either security is traded off/compromised for better overall performance or vice versa. To achieve this goal, quantitative tools are needed to model, evaluate and optimise the trade-off between security and performance.

In order to accurately model and evaluate this trade-off under bursty traffic, performance and security mechanisms should be modelled in an appropriate way besides the use of proper traffic models for traffic variability together with the defining of suitable performance and security metrics which play a vital role in the evaluation and optimisation process. Several studies in the literature [2 , 4 , 5 , 7 , 8 , 9] state that high-speed network traffic exhibits bursty behaviour; therefore, including this assumption in the model makes it more realistic.

This thesis develops an effective quantitative methodology for the analysis of arbitrary queueing networks (QN) models and Generalised Stochastic Petri Nets (GSPNs) through Discrete-Event Simulation (DES) and extended applications into performance vs. security trade-offs involving infrastructure and infrastructure-less high-speed networks under bursty traffic conditions. Specifically, investigations are carried out focusing, for illustration purposes, on high-speed network routers subject Access Control List (ACL) and also Robotic Ad Hoc Networks (RANETs) with Wired Equivalent Privacy (WEP) [10] and Selective Security (SS) (c.f.,[11]) protocols, respectively. Burstiness of traffic is

reflected within each case by using Generalised Exponential (GE) distribution[12] as inter-arrival and service times which enables the evaluation and prediction of pessimistic ‘upper bounds’ for the performance of the secure networks.

In the context of a router with ACL mechanism representing an infrastructure network node, performance degradation is caused due to high-speed incoming traffic in conjunction with ACL security computations making the router a bottleneck in the network [3] and this considerably affects the overall performance of the high-speed network. To quantify and predict the trade-off of this degradation, the proposed quantitative methodology employs a suitable QN models for router with ACL.

These queues have single or quad-core CPUs with multiple-classes and correspond to a security processing node and a transmission forwarding node. First-Come-First-Served (FCFS) and Head-of-the-Line (HoL) are the adopted service disciplines together with Complete Buffer Sharing (CBS) and Partial Buffer Sharing (PBS) buffer management schemes. The mean response time and packet loss probability at each queue are employed as typical performance metrics. Numerical experiments are carried out, based on DES, in order to establish a balanced trade-off between security and performance towards the design and development of efficient router architectures under bursty traffic conditions.

The proposed methodology is also applied into the evaluation of performance vs. security trade-offs of RANETs with mobility subject to WEP and SS protocols. WEP protocol is engaged to provide confidentiality and integrity to exchanged data amongst robotic nodes of a RANET and thus, to prevent data capturing by unauthorised users. WEP Security mechanism in RANETs, as Infrastructure-less networks, is performed on each single node, subject to traffic burstiness as well as nodal mobility. In this context, the proposed quantitative methodology is extended to incorporate an open QN model of a RANET with Gated queues (G-Queues), arbitrary topology and multiple classes of data

packets with FCFS and HoL disciplines under bursty arrival traffic flows characterised by an Interrupted Compound Poisson Process (ICPP). SS is included in the Gated-QN (G-QN) model in order to establish an 'optimal' performance vs. security trade-off. For this purpose, performance engineering Principles (PEPs), such as the provision of multiple classes with HoL priorities and the availability of dual CPUs, are complemented by the inclusion of robot's mobility, enabling realistic decisions in mitigating the performance of mobile robotic nodes in the presence of security.

The proposed quantitative methodology is further enhanced by formulating a theoretical hybrid framework to capture 'optimal' performance vs. security trade-offs for each node of a RANET by taking more explicitly into consideration security control and battery life. Specifically, each robotic node is represented by a hybrid Gated GSPN (G-GSPN) and a QN model, thus the framework is named G-GSPN_QN. In this context, the G-GSPN models bursty multiple class traffic flows, nodal mobility, security processing and control whilst the QN model has, generally, an arbitrary configuration and reflects 'intra'-robot (component-to-component) communication and 'inter'-robot transmissions through arbitrary QN consisting of finite capacity channel queues. Two theoretical case studies from the literature are adapted to illustrate the utility of QN towards modelling 'intra' and 'inter'-robot communications. Moreover, Extensions of Combined Performance and Security Measure (CPSM) metric proposed in the literature [13] are suggested to facilitate investigating and optimising RANET's performance vs. security trade-offs.

1.2 Motivation

Due to its significance, performance and security trade-offs modelling and evaluation in high-speed networks, which exhibit bursty behaviour, has been investigated in the literature using different approaches. Activating security mechanisms causes performance (quality) degradation such as increasing processing and transmitting times. Such degradation should be quantified in order to determine application specific parameters and model network traffic

flows towards improving Quality-of-Service (QoS) [14]. This quantification can be made through designing/proposing “Model-based quantitative technique” [15]. Several studies exploited models such as QNs and GSPNs, to quantify security impact and then explore the trade-off between performance and security [6 , 13 , 14 , 15]. For the best of the author knowledge, Zorkadis [6], in 1994, was the first to propose a quantitative modelling of security trade-off for three nodes connected in tandem, using QNs in infrastructure network. Security is modelled implicitly where the service rate were assumed to be less when security mechanism is activated. The metric used in this study is pure performance metric, which is End-to End Mean Response Time that is used implicitly to show how to trade off between performance and security. Meanwhile, in 2008 Cho [15] introduced the concept of security trade-off for infrastructure-less network, i.e., a group of Mobile Ad Hoc Networks (MANETs) nodes, using Stochastic Petri Nets (SPNs). Moreover, the author used Mean Time To Security Failure (MTTSF) as a security metric in addition to the Mean Response Time, R, as a traditional performance metric to indicate the improvement of the performance and security trade-offs. In 2010, Wolter and Reinecke [13] proposed a combined performance-security model for an abstract communication system, based on GSPN, in order to evaluate and optimise the trade-off between performance and security by means of CPSM concept which was introduced for the first time to enable simultaneous optimisation of performance and security in terms of one metric. However, these models do not take into consideration performance engineering principles and the adverse impact of traffic burstiness and security protocols on performance on the network.

In this thesis, burstiness of traffic is reflected by utilising GE distribution as inter-arrival and service times which enables predicting ‘Upper bounds’ for the performance-related security.GE distribution [12] is used to model inter-arrival and service times at each node in order to capture the traffic burstiness of the network and predict pessimistic ‘upper bounds’ of network performance.

1.3 Aims and Objectives

The main aim of the research presented in this thesis is to develop an appropriate model-based quantitative approach to assess the performance and security trade-off for infrastructure and infrastructure-less high-speed networks subject to bursty traffic, based on individual QNs and combined QNs and GSPNs associated with performance metrics and combined performance and security metrics. These objectives include the following aspects:

1. To use QNs and GSPNs quantitative analysis tools to model and quantify and mitigate security impact as well as performance security trade-offs in communication networks;
2. To use the GE distribution to reflect traffic burstiness, and to simulate it within DES as a random generator;
3. To utilise and extend the existing security and performance metrics as well as combined performance and security metrics;
4. To design and construct a simulation program in Java for an open G-QN model with multiple classes and multiple servers subject to FCFS and HoL discipline;
5. To propose a hybrid G-GSPN_QN framework and design a QN model for intra and inter-robot communications.

1.4 Contributions

This work establishes quantitative guidelines for the design and development of an effective quantitative methodology for the analysis of arbitrary QN models and GSPNs through DES and extended applications into performance vs. security trade-offs involving infrastructure and infrastructure-less high-speed networks under bursty traffic conditions. Specifically, investigations are carried out focusing, for illustration purposes, on high-speed network routers subject ACL and also RANETs with WEP and SS protocols, respectively.GE-type random variable has been simulated by utilising the fact that GE is a limiting case of Hyperexponential distribution (H_2) by applying the approximation

algorithm of proposed in [12]. This GE variable is then used in the simulation program of open QN model to model inter-arrival and service times.

In the first case study, a proposed quantitative QN node model subject to multiple classes FCFS and HoL discipline together with CBS and PBS. Repetitive Service-Fixed Destination blocking mechanism (RS-FD) [16] is exploited to reflect the behaviour of ACL mechanism. Security is modelled implicitly and explicitly as suggested by Zorkadis [6] and Saleh and Alkhatib[14] respectively. Traffic burstiness is captured by the use of GE as inter-arrival and service times, which enables the prediction of 'Upper Bounds' for the performance-related security.

The second case study focuses on the trade-off between performance and security in RANETs, whose security functions are based on the WEP security (c.f., [10] and SS protocols (c.f., [11], [17]) at each robotic node. Security is modelled by an explicit QN node connected in tandem with another QN node for transmission. To make the model more realistic, the node's mobility is reflected by the use of G-Queues, proposed in [18], to form an Interrupted Poisson Process (IPP) (c.f.,[19])input to the queue, which is connected to the security node. The case study considers an arbitrary stable open G-QN with infinite capacity, multiple FCFS and HoL classes and bursty GE inter-arrival traffic flows(c.f., [20]) characterised by an ICPP(c.f., [19]).

The proposed quantitative methodology is further enhanced by formulating an advanced hybrid framework for capturing 'optimal' performance vs. security trade-offs for each node of a RANET by taking more explicitly into consideration security control and battery life. In particular, the framework is composed of GSPNs and QNs with arbitrary topology and multiple classes subject to FCFS and HoL discipline. Two theoretical case studies from the literature [21 , 22 , 23] were adapted to illustrate the utility of QN towards modelling intra-and inter-robot communications. Two extended CPSMs based on the one proposed in the literature (c.f., [13]) are suggested to evaluate and optimise the trade-off.

Note that DES methodology involves simulating an open QN model with multiple classes and multiple servers with Gated queue subject to FCFS and HoL finite capacity queues with RS-FD blocking mechanism (c.f., [16]) where the inter-arrival and service times with GE distribution.

1.5 Thesis Organisation

Chapter 2 reviews high-speed networks and performance and security trade-offs fundamentals.

Chapter 3 surveys previous work on network traffic models used to capture burstiness in high-speed networks namely: IPP, GE and ICPP.

Chapter 4 introduces quantitative techniques used to assess the trade-off between performance and security, in particular, QNs, GSPNs or combination of both and use in modelling and evaluating the trade-off.

Chapter 5 it presents the proposed QN model for the high-speed router with ACL security mechanism which is modelled both implicitly and explicitly using QN under bursty traffic conditions. The performance-related security of the router is evaluated through appropriate performance metrics.

Chapter 6 it introduces the proposed G-QN model for RANETs with WEP with SS security protocol where security is modelled explicitly within the QN as an individual node. Mobility of RANETs is reflected in the QN model with a Gated Queue, as proposed in [18].

Chapter 7 presents the proposed hybrid G-GSPN_QN modelling framework of RANETs in order to overcome some of the inherent limitations of individual QN and GSPN models. Two case studies are presented to reflect the utility of QN to model ‘intra’-robot component to component and ‘inter’-robot to robot communication. In addition, it presents three extended CPSMs that can be adopted to investigate an enhanced combined optimisation of performance vs. security trade-off in RANETs. Note that a detailed explanation of simulating GE-

type random variable besides the main simulation building models used in chapter 5 to 7 are included in appendices A to G.

Chapter 8 summarises the contributions of this thesis and makes some recommendations for future work.

Chapter 2 Performance and Security Trade-offs in High-Speed Networks

2.1 Introduction

It is important to design secure and reliable networks of greater capacity that support high-volume traffic that exhibit burstiness behaviour [4 , 9 , 24]. Towards achieving this goal, modelling and evaluating performance and security parameters is needed in order to evaluate and predict future traffic volumes [4]. It is not feasible to meet performance and security requirement simultaneously as they affect each other [5], thus it is vital to trade them off.

This chapter presents the classifications of high-speed networks with a focus on routers and RANETs as examples. It then describes performance and security concepts and their metrics and showing how security services affect the network's performance. Determining this impact is required to identify the concepts of security and performance trade-off.

2.2 The Classification of High-Speed Networks

High-speed network can provide high-speed support to meets the requirements of transfer speed and access time over limited distances [25] and they now dominate both local area networks (LAN) and wide area networks (WAN) markets. The most important of them are as follows:

2.2.1 Infrastructure High-Speed Networks

In infrastructure networks, the network services are provided to all nodes by particular servers which are responsible for assigning addresses and routing. The connection between these servers and nodes is made via wired or wireless channels [26]. Main types in this category are [4]:

1. Fast Ethernet and Gigabit Ethernet;
2. Fibre Channel;
3. High-Speed Wireless LANs.

High-speed router is an example on this type of networks and it represents a linking device that provides security access control.

a) High-Speed Routers

A router is an access control device in infrastructure networks, among other devices (such as firewalls, switches, gateways). Routers perform traffic filtration based on the predefined routing criteria, to protect the network components (c.f., [27]. This can be achieved by testing the packet's headers and rerouting the traffic accordingly. An incoming packet is either forwarded to its destination (or next node) or dropped [3].

From a performance point of view, ACL security mechanism running on the router consumes the router's CPU usage [3]. Thus, there is a need to trade off between its performance and security.

2.2.2 Infrastructure-less High-Speed Networks

In infrastructure-less networks, communicating nodes should group themselves and provide routing and security services via multi-hop transmissions. Each node acts as a router [26]. This category includes WLAN with infrastructure-less, i.e. ad hoc networks. Such networks provide services and coverage of locations that are difficult to wire [4].

A robotic mobile wireless ad hoc network (RANET) is an example on this type of networks and nodes within this network need to perform security encryption in order to protect their data.

b) RANETs

RANET allows robots to form wireless ad hoc network in order to exchange data among them. RANETs seem to have a most suitable architectural platform to support the dynamic nature of robotic applications (c.f., [28 , 29]). Robots are usually equipped with low-power wireless transceivers with short range enabling them to communicate only with close neighbours. The ad hoc environment of RANETs is cost-effective and requires fewer resources. Moreover, decentralized control in RANETs is a most suitable mechanism as it shows the

robustness of robot nodes to local failures and self-organisation, scalability and a wide range of applications. To this end, MANETs qualify as a most suitable choice for RANETs as the dynamic topology of MANETs supports mobility, self-organisation and control without infrastructure which enable nodes to communicate over wireless channels without the presence of a fixed infrastructure (c.f., [29]). Robots can be '*tele-operated'* where a human controls their operation through the network or '*autonomous'* where robots exchange data through the network without human interaction. Robots among the RANET might be heterogeneous in terms of sensory skills, mobility and robot's architecture (c.f., [30]).

a) Typical Components of a Robot

A typical robot may contain five fundamental units as following [31 , 32]:

1. *Controller*

It controls and processes the operations of robot mechanical parts by means of determining the appropriate signals to the actuators in order for the robot to perform the required tasks.

2. *Sensing Unit*

This unit gives information about the environment 'External purpose sensor', or the robot itself 'internal purpose sensor'. 'Internal sensors' monitor the various parts of the robot, e.g., monitoring robot's speed. 'External sensors' such as cameras and range sensors used to sense external data (e.g., video and distance measurements) and used by the controller to move the robot 'Intra-robot' or shared with other robots 'Inter-robot' and communications.

3. *Power Unit*

This unit deals with the energy consumption within the robot node where it is associated with all hardware components. The level of power decreases depending on the draw made by these components.

4. *Transmission/ Receiving Unit*

It includes the transmitter and receiver (which are known as transceiver) within the robot to send and receive data.

5. Actuators

These components are either mechanical or electric devices, such as motors and joints (which connects the parts of a robot's arm to allow them moving in different directions). Actuators are controlled by the robot to create the required motion as a response to regulating signals from the controller [31]. The overall operation control of a robot involves three steps: namely: sensing, processing and action (c.f., [31]), as depicted in Figure 2-1.

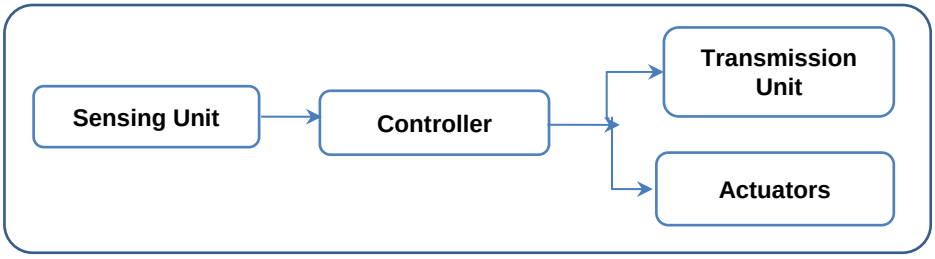


Figure 2-1 Intra-robot communications (adapted from [31]).

2.3 Performance

High-speed networks require data buffering and higher computation power to support high performance distributed computing [25]. The performance of such networks is rapidly degraded due to the gap between the high network speed and the traversed hardware according to Moore's law (c.f.,[3 , 9]). Thus, it is vital to assess this degradation and work towards improving the overall performance of the network. For the purpose of performance evaluation, QoS metrics that indicate the network performance are introduced.

2.3.1 Metrics

Performance metrics help in prioritising the use of network's resources according to the required application, e.g. real-time audio or video transmission [33]. It is worth mentioning that when a network with multiple class is considered, the performance metric per class is known as a 'Marginal metric' while the overall performance metric is called an 'Aggregate metric' [34].

The most commonly used metrics in high-speed networks are as follows:

1- Mean Response Time (W)

This is the amount of time taken by the network device/node to process a message [2 , 33].

2- End-to-End Delay

End-to-end delay is defined as the total delay seen by messages or data packets that traverse the network from a source node to a destination node and includes processing delay, packetisation delay, transmission delay, queueing delay (c.f., [35]).

3- Packet Loss Probability (PLP)

This is the percentage of messages that are blocked/lost on arrival if the linking device node is at full buffer capacity [2].

4- Mean Queue Length (MQL)

This represents the mean number of messages in the buffers waiting to be served [34].

5- Utilisation (U)

This specifies the fraction/percentage of time required by the linking device/node to successfully process messages [33].

6- *Throughput*

Throughput is a measure of the amount of data (number of messages or data packets per unit of time) transmitted between two nodes in a given period of time [4].

7- Power Consumption

Power metrics assess power consumption and its progressive reduction power-constrained networks [29]. Power metrics can be either ‘Explicit’ (c.f.,[36]) in which power is represented by the consumed power per bit (or byte) transmission, or ‘Implicit’(c.f., [37 , 38]) which are defined in terms of the network’s lifetime.

The following section introduces security service besides the relationship between these services and possible attacks against them. Finally, types of performance degradation caused by such services are outlined.

2.4 Security

In this section security services and attacks are described.

2.4.1 Security Services

A security service is the collection of mechanisms implemented to reduce the risk associated with threats [33]. The main services are Integrity, Access control, Confidentiality and they are needed to secure exchanged data in infrastructure networks (e.g., in routers and servers), or in individual nodes in infrastructure-less networks [39]. The following section gives a brief description of each service.

1. *Integrity Services*

This service helps to ensure that the network messages are not modified by unauthorised parties [33 , 40].

2. *Access Control Services*

This service ensures that only authenticated users who have specific authorisations are able to access particular resources [33 , 39 , 40].

3. *Confidentiality Services*

Confidentiality ensures that network data are not visible to unauthorised parties [40 , 41] and they are based on cryptographic algorithms. Security services and their corresponding performance costs are summarised in Table 2-1.

Table 2-1 Security services and their performance costs (adapted from [6])

Security Services	Performance Costs
Access Control	Computation costs before and during information transfer stage.
Confidentiality	Computations/ processing costs at the end nodes (in end-to-end encryption) or at intermediate nodes.
Integrity	The expansion of the message length besides the computation costs (due to computing and appending Cyclic Redundancy Checks (CRC) to the message)

2.4.2 Attacks

Attacks on high-speed networks cause damage to the stored or transmitted information. There are two main types of attacks (for wired and wireless networks) [40 , 41]:

1. Access

An access attack is an attempt to gain access to the stored or transmitted information that the attacker is not authorized to read. This type of attack is an attack against **the confidentiality** of the information.

2. Modification

This is an attempt to modify stored or transmitted information that an attacker is not authorised to modify. This type of attack is an attack against the **integrity** of the information. The relationships between security attacks and security services are shown in Table 2-2 (c.f.,[40]).

Table 2-2 Security services (adapted from [40])

Security Service		
Attack	*Confidentiality*	*Integrity*
Access	×	
Modification		×

2.4.3 Metrics

Unlike performance, it is not possible to measure security directly (c.f., [42]). However, by considering security as a ‘Process’, it can be quantified and linked with reliability” [43]. Reliability is related to the internal functionality of the system thus faults can be fixed based on pre-knowledge, while security protects the system against external attacks, which are not predictable. In this context, “measuring security is often similar to measuring reliability” (c.f., [13]). From this perspective, some credible security metrics may be defined as follows (c.f., [13 , 42]):

1. “The mean time to Incident Discovery (~corresponds to Mean Time to Failure in reliability)”;

2. “The Mean time taken to recover from an attack (~corresponds to Mean Time to Repair in reliability)”;

Wolter and Reinecke [13], on the other hand, defined some security metrics for a general encryption system in terms of the “probability of being in a certain condition, namely the following [13]:

1. “The probability of the encryption key being valid”;
2. “The probability of an undetected broke key” (i.e., the percentage of the amount of sensitive information leakage at a node).

Moreover, several security metrics related to particular security mechanisms like cryptographic algorithms can be used such as ‘Encryption key length’ proposed for MANETs in [44].

In addition, some CPSMs were suggested by Wolter and Reinecke [13] in order to allow system designers to quantitatively determine acceptable trade-offs between performance and security. This can be made by assessing the degree of protection provided by security mechanisms at an acceptable level of performance (e.g., [13]).

2.5 Trade-off between Performance and Security

When the security is activated, to what extent will the network performance be affected? And is such degradation acceptable for the real-time applications in high-speed networks? In order to answer such questions, a trade-off between performance and security needs to be explored and this will help in[45]:

1. Increasing the understanding of secure systems’ behaviour;
2. Facilitating the evaluation of the adverse impact of security on performance and predicting its future behaviour;
3. Performing quantitative evaluation of the secure systems being designed, thus leading to their optimisation.

2.5.1 Approaches of Trade-off Evaluation

Trading off between performance and security involves either compromising/ trading off security, in terms of security metrics, for better overall performance,

indicated by the performance metric, or vice versa. The performance-related security can be evaluated firstly by modelling performance and security accurately using effective quantitative modelling tools which include QNs and GSPNs and they have various features in terms of simplicity and modelling power. It is also significant to define suitable metrics for both performance and security as well as appropriate combined metrics/ functions [13].

This thesis suggests exploiting PEPs to optimise the performance of secure networks, which may or may not require hardware upgrades. Some approaches need hardware upgrades are such as multiple-core CPUs with higher speeds. While those do not required such upgrades are such as selective security [46] and space priority, service priority [16]. In this context, the scale of performance improvement is of significance.

2.6 Case Studies Considered

In both considered case studies, the adverse impacts of access control and encryption services are taken into consideration in routers and RANETs respectively.

2.6.1 High-Speed Routers and ACLs

In this section, brief descriptions to ACL mechanism besides Attacks on routers that can be prevented by ACL are provided [3]. ACL used to filter traffic entering or leaving an interface and it consists of a set of commands (i.e., list of security protections [47]) that define specifically which traffic flows are permitted and denied[47]. There are two types of ACL; ‘Standard’ and ‘Extended’ [48]. In standard ACL, the filtration is made according to the source IP address. While in extended ACL, which is most advanced, filters incoming/ outgoing traffic based on several parameters such as source IP address, destination IP address, the protocol used and port numbers as shown in Figure 2-2.

ACL can either check inbound (i.e., incoming) or outbound (i.e., outgoing) traffic thus ACL can be further classified to ‘Inbound ACL’ and ‘Outbound ACL’. More information about ACL classifications can be found in [39 , 47 , 49].

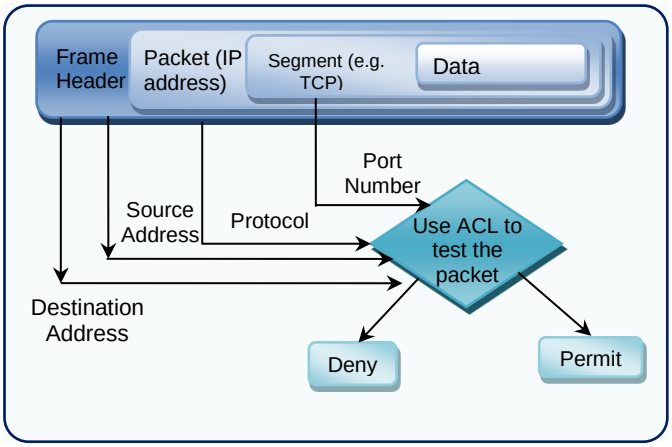


Figure 2-2 The concept of ACL mechanism in the router (adopted from [47])

a) Attacks on High-Speed Routers

Some of possible attacks against routers include “unauthorised access, rerouting, denial of service (DoS), and eavesdropping and information theft” (c.f., [27]). ACL security mechanism can detect and prevent several access attacks on routers, such as "Address Resolution Protocol (ARP), spoofing attacks, DoS attacks through filtering malicious traffic from the internal” (c.f., [27]).

b) ACL Security Application Vs. CPU Performance

The filtering process performed by ACL in a router - from the performance prospective - introduces computation costs during data transmission (c.f., [6]). Consequently, there is a need to reduce the “speed gap” [3] between bandwidth and the processors at the router which may make it a bottleneck in the network. When ACL is activated, the router’s CPU usage is consumed. To reduce this effect, a multi-core processor can be used for this purpose.

c) Multiple-Core CPUs

A multi-core processor composed of two or more individually attached cores which are typically integrated into a single integrated circuit chip [50]. A multi-core processor does not often need a new motherboard since it can use existing boards that feature the correct socket [51].

2.6.2 RANETs and WEP

Due to the fact that data exchanges among RANET nodes take place through an open medium, communications may be interrupted and easily captured by unauthorised users. To eliminate this impact, encryption algorithms such as WEP and Wi-Fi Protected Access (WPA) can be utilised (c.f., [15 , 52]). Attacks against RANETs and how WEP can reduce their effect are described below.

a) Attacks on RANETs

Possible attacks against RANETs can be either: 'Passive attacks', in which data can be read by the attacker) without being modified, or 'Active attacks' where data can be modified, thus leading to congestion. Consequently, this type of attack is more serious and should be detected as soon as it occurs. This can be performed using encryption mechanisms.

b) WEP Protocol

WEP provides confidentiality and integrity of stored and transmitted data (c.f., [10]). WEP encrypts data using a shared WEP secret key and it utilises CRC checksum for integrity. WEP offers a quite low level of security thus it can be cracked easily (c.f., [10]) but it is considered in this study to illustrate security modelling concepts in infrastructure-less networks. From the performance point of view, WEP involves employing extra bits to secure packets and consequently requires additional processing time, power to perform encryption (c.f., [10]). The performance of WEP can be enhanced via SS (c.f., [11]).

c) SS

To mitigate the adverse effect of security on network performance, SS mechanism, proposed in (c.f., [11]), can be used where only a percentage, p, of packets, where ($0 \leq p \leq 1$), are allowed to go through the security process to guarantee the acceptable levels of security in RANETs within required bounds of performance as well as power-saving in MANETs (c.f.,[11 , 17 , 46]).

2.7 Summary

This chapter introduced the concept of high-speed networks and the significance of modelling and evaluating trading off between their performance and security. It also investigated the concept of security services and mechanisms and how they affect performance in communication networks. In addition, some commonly used metrics for performance and security have been briefly reviewed. In the following chapter, network traffic flows models will be introduced.

Chapter 3 Modelling Networks Traffic Flows

3.1 Introduction

The design of secure High-speed networks which run various applications and security services under bursty traffic is challenging [53]. To facilitate this task, it is important to investigate traffic models of the network to avoid QoS degradation. Such models should accurately evaluate and predict the network's performance and security and to helps in mitigating the adverse impact of security on the system's performance. Therefore, traffic models are an essential part of the performance evaluation of the network (c.f., [5 , 53]). This chapter reviews the traffic models used to reflect bursty traffic in high-speed networks.

3.2 Traffic Characteristics

The impact assessment of heterogeneous traffic flows on the performance-related security of a high-speed network is one of the current key research issues in the field (c.f.,[54]). Once the traffic characteristics are better comprehended and credibly modelled, they may provide a strong basis for performance and security trade-off evaluation and optimisation (c.f., [55 , 56]). Moreover, networks' best/worst-case scenarios can be identified for certain applications. This section provides an overview of traffic models that capture traffic burstiness. It also describes how such models have been used in this study for high-speed networks in general and for RANETs in particular.

There are three important characteristics of a traffic source and they are as follows [57]:

1. **Traffic Average Data Rate**

It gives an indication of the expected traffic volume for a given period of time.

2. **Traffic Burstiness**

Burstiness describes the possibility of messages arrival in bulk/batches (i.e. in groups instead of individual arrivals). Considering burstiness is vital since it can predict the situations in which network congestion and loss of data occurs. Most traffic sources supported by high-speed networks are highly bursty (c.f., [24]).

Note that traffic studies in high-speed networks only mean and variance may be relied on and thus GE distribution which is completely defined in terms mean and variance implies least bias [16].

3.3. Traffic Models

Traffic describes and generates telecommunications traffic, which is important for two main reasons:

1. Describing traffic flow to the service provider; thus, new connections with a specific QoS, such as achieving a given level of security) can be admitted without affecting other connections;
2. Making new designs for future networks through the modelling of these networks and predicting their performance and security besides applying the traffic type to be tested [57].

The main arrival processes considered in this thesis for high-speed networks include IPP, Compound Poisson Process (CPP) and ICPP, which are stochastic process (i.e., random functions of time). These processes and some corresponding inter-arrival time distributions are summarised below:

3.3.1 IPP

An IPP traffic flow (c.f., [19]) is a modified Poison traffic process with two states, 'On' and 'Off', as in Figure 3-1. In the 'On' state, traffic is generated according to Poisson process, while no traffic is generated in the 'Off' state. Thus, the 'On' and 'Off' periods are exponentially distributed with means of 1/β and 1/ α respectively. IPP may be seen as a 2-state Markov Modulated Poisson Process (2- MMPP), where the mean arrival rate λ_2 at 'Off' state is zero (c.f., [58]). IPP has been used to present voice, data and video transfer over the Internet. In the context of this study, the IPP will be used to model the wireless channel availability between a pair of communicating RANET nodes (c.f., [18 , 59]).

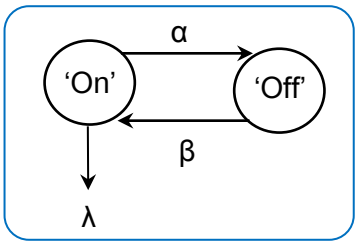


Figure 3-1 The IPP traffic model

3.3.2 CPP

A stochastic process (X(t), t ≥ 0) is called a CPP process when it can be presented by (c.f., [60]):

$$X(t) = \sum_{i=0}^{N(t)} Y_i, t \geq 0 \qquad \text{Eq. 3-1}$$

Where (N(t), t ≥ 0) is the counting process for Poisson process and Y_1, Y_2, . . . are independent, identically distributed random variables with discrete distribution represents the batch size that arrived at time t and they are independent of (N(t), t ≥ 0). When the batch size is geometrically distributed, the CPP is the counting process of a GE-type inter-event time distribution, which is described below:

a) GE Distribution

GE distribution is determined by (c.f., [12 , 20]).

$$F(t) = P(W \leq t) = 1 - \tau e^{-\tau\lambda t}, t \geq 0 \qquad \text{Eq. 3-2}$$

where $\tau = \frac{2}{(C^2+1)}$, W is the random variable, an inter-event time, and $(1/\lambda, C^2)$ are, respectively, the corresponding mean and squared coefficient of variation (SCV) defined by:

$$C^2 = \frac{Var(W)}{E^2(W)} \qquad \text{Eq. 3-3}$$

C^2 gives an indication of degree of the burstiness of the inter-arrival and service time completion. The GE-type distribution is shown in Figure 3-2.

GE can also be interpreted as 'extreme case' of the family of two-phase Hyperexponential-2 (H_2) having the same λ and C^2, where one of the two phases has a very large mean rate (i.e., zero service time). In this context, GE

model defines the 'Upper' performance bounds for the corresponding solutions based on two-phase H_2 distribution with the same first two moments [12 , 20] (c.f., Appendix B).

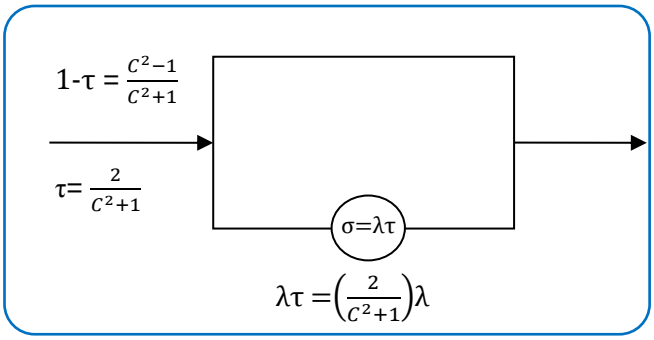


Figure 3-2 The GE-type distribution with parameters τ and σ (c.f., [12 , 20])

Over the years, GE has been linked with bursty traffic flows and variable service times (c.f., [20], [16]). GE is the most appropriate distribution to model simultaneous arrivals of messages, generated by bursty traffic sources to a secure node in a high-speed network [16].Traffic burstiness impact can be assessed by increasing values of the SCV of inter-arrival times, $C^2 (C^2>1)$.

a) The relation between IPP and GE

IPP can be fitted according to the inter-arrival time process into H_2 distribution as proposed in [61 , 62]. H_2, in turn, can be approximated to GE when the tuning parameter k of $H_2 \rightarrow \infty$ (c.f., [20]) (c.f., Appendix B for more details). Thus, IPP can be expressed in terms of GE parameters and this feature can be utilised in the context of the proposed performance and security trade-off framework for mobile RANETs (c.f., chapter 7), where IPP represents a Gate in G-queue to reflect a node's mobility (c.f., [18]). GE then can express the inter-arrival times of messages to enable predicting 'upper bounds' of networks performance in the presence of security.

3.3.3 ICPP

The ICPP (c.f., [58]), shown in Figure 3-3, is similar to an IPP except that the inter-arrival time within the 'On' state follows the GE-type distribution with mean

rate λ and SCV, $C_a^2 > 1$, i.e., traffic in the 'On' state is generated according to CPP, whilst no traffic is generated in the 'Off' state.

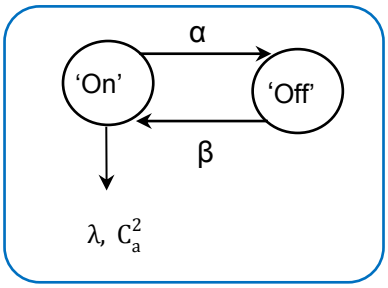


Figure 3-3 The ICPP traffic model

3.4 Traffic Modelling for RANETs

Poisson process was used as arrival processes in MANETs in (c.f., [18 , 63]). Since this assumption is not realistic to reflect bursty traffic, CPP may be adopted instead to model the inter-arrival and transmission times in MANETs (c.f., [64], [65]). Other traffic modelling studies and load distribution in MANETs can be seen in [18 , 56 , 59 , 66 , 67 , 68].Several approaches to mobility using QNs for MANETs employ IPP to capture the link state between a pair of communicating nodes such as the proposed Gated Queue (G-Queue) by Bhatia et al.(c.f.,[18 , 59]). Under certain conditions, these studies may be applicable to RANETs (c.f., [64]).

3.5 Summary

This chapter reviewed most commonly used traffic flows models in high-speed networks to reflect their traffic burstiness nature. These models are such as IPP and ICPP. Once credibly modelled, these models will help in providing a strong basis for performance and security trade-off evaluation and optimisation (c.f., [55 , 56]) as well as determining the networks' best/worst-case scenarios.

The following chapter describes in detail the network modelling and evaluation tools and how they have been used to model and assess the trade-off between performance and security.

Chapter 4 Network Modelling and Evaluation Tools

4.1 Introduction

Network modelling and evaluation tools are needed to provide a way of exploiting traffic models as their input; they then produce a response that mimics the behaviour of the system being modelled. The main purpose of using these tools is to provide 'Worst-case' scenario evaluations for system designers [53]. Appropriate models are beneficial to assess and predict the suitability of new security protocols under different requirements prior to the actual implementation. This chapter reviews the most common network modelling and evaluation tools which are QNs, GSPNs, and combined QNs and GPSNs, to capture the behaviours of the network and evaluate its performance-related security.

4.2 Network Evaluation Tools

There are three ways of evaluating the performance and security trade-offs in high-speed networks:

1. The measurements of a tested version (or prototypes of the system) of the system instead of the system itself, which is more expensive;
2. The implementation of a mathematical model that describes the system's behaviour through equations and constraints. This approach is used when it is not feasible to build the system's prototype. QNs, PNs and generalisations can be used in this context to model secure systems and Maximum Entropy (ME) [12] principle can be used to analyse a network on QNs;
3. The simulation of the system, in which a computer program is built to mimic the behaviour of the system. Simulation is used when the system to be evaluated is too complex or does not exist [45].

Since the implementations and performing of measurement-based evaluation are expensive and the performed tests are time-consuming, a model-based evaluation is more appropriate thus, it has been chosen in this study.

The model-based tools to evaluate the trade-off between performance and security are as follows:

1- Queueing Networks;

2- Petri Nets (PNs) and Generalisation.

Simulation models composed of QNs have been used to evaluate the performance and security trade-offs. The following section presents a more detailed description of these techniques and their use in the literature to model security and performance-related security [45] in infrastructure and infrastructure-less networks.

4.3. Modelling Network Tools and Performance vs. Security Trade-offs

Fundamentals of QNs, PNs and generalisations are introduced in subsections 4.3.1 and 4.3.2, respectively, in conjunction with their quantitative modelling applications on the evaluation of performance vs. security trade-offs (c.f., Table 4-1 based on:

i) an open QN for generic networks and Gated QN (G-QN) model of a RANET [69], and

ii) an SPN model of a general communication network [13] and a GSPN of a MANET [15].

Table 4-1 Modelling of performance vs. security trade-offs

Security Modelling	**Performance-Security Modelling**
• **Generic Networks** QNs [6 , 14 , 65], PNs [13 , 41 , 70]; • **MANETs** QNs [14 , 71]), SPNs [72 , 73].	• **Generic Networks** QNs [6 , 74]), GSPNs [13 , 41]; • **MANETs** QNs [64 , 69]), SPNs [15].

Other approaches, besides QNs and GSPN quantitative models, have been considered in the literature to assess the trade-off between performance and security in the context of encryption-related security in wireless networks [46 ,

75 , 76] and networked control systems (c.f., [77 , 78 , 79]) and these approaches are out of the scope of this thesis.

4.3.1 QNs

In this section, the fundamentals of QN models and their use in modelling security services and performance-security trade-off are presented.

a) Fundamentals of QN Models

QNs are quantitative tools for modelling complex systems through a “concise graphical description” (c.f.,[80]) of service centres, queues and their disciplines besides routing amongst these nodes (c.f., [81]). A QN may be either ‘Open’, with an external arrival process generated by an infinite population source, or ‘Closed’ with a fixed number of messages or ‘Mixed’ open and closed (c.f.,[82 , 83]). In the context of this thesis, only open QNs are considered since external arrivals to the router/RANET nodes are expected to be secured and processed then they depart from the network.

QNs may take into consideration scheduling strategies and priority rules, such as FCFS, in which all traffic flows have the same service priory, and HoL, where jobs are divided into classes and these with higher priority are served first [4 , 34]. Low priority classes are not pre-empted from the queue server upon the arrival of high-priority class (c.f., [16]). QNs also have either single or multiple channel queues with infinite or finite capacity and, thus, blocking. [84].

b) Buffer Management Schemes

Buffer Management Schemes [16] provide space priority such as CBS and PBS. Under CBS, jobs from any class can join a finite capacity queue whenever there are free spaces for them. While in PBS, a threshold is set to allow high-priority class jobs to occupy the whole capacity while those with lower priority classes can only join the queue if the total number of jobs in the queue is less than a threshold value.

c) RS Repetitive services (RS) Blocking Mechanism

According to this mechanism [16 , 85], if a job completes service at queue i and attempts to join queue j but upon arrival, it finds queue j at full capacity, then the

job is rejected and immediately goes back to receive another service at queue i. This action is repeated until the job completes a service at node i at the time the destination node j is not full. There are two types of RS which are RS with Fixed Destination (RS-FD) and RS with Random Destination (RS-RD). In RS-FD, the destination node j to which the job is routed is determined after the first service and it cannot be modified (changed) later. While for R*S-RD,* the destination node j, is selected at each service completion in an independent way of the one chosen previously.

The main advantage of QNs is their ability to model the interaction between a system's resources and its applied workload and they are acceptable whenever the required level of detail for the model specification is not too high (c.f., [86]), and they can effectively represent single and multiple servers with priority and non-priority service disciplines and multiple classes under various blocking mechanisms [16 , 20 , 87].However, QNs are not quite suitable for capturing more complex operations such as synchronisation of processes, software contention and concurrency (c.f., [81 , 83]).

d) Security Modelling Using QNs

Security can be either modelled implicitly or explicitly.

i) Security Implicit QNs

An earlier open QN model was proposed by Zorkadis in [6], depicted in Figure 4-1, for the evaluation of performance vs. security trade-off in a general communication system with two linked firewalls through a wired channel. More specifically, two firewalls connected in tandem, via the communication channel, were modelled and analysed in [6], each of them having a stable M/G/1 queueing system under FCFS discipline. Security functions (encryption, integrity and authentication) were modelled implicitly by means of reducing the overall mean transmission rate of the server at each M/G/1 queue.

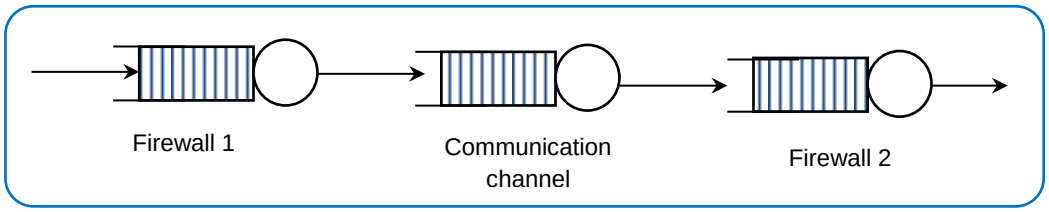


Figure 4-1 The communication system modelled by Zorkadis [6]

In this study [6], the impact of bursty traffic was not taken into consideration. Moreover, either a single queueing node or queues in tandem with one arrival class were investigated in the trade-off.

ii) *Security Explicit Queueing Models*

QN model was employed in [14] for the performance and security trade-off analysis of a static single MANET node, subject to the WEP security protocol (c.f., Figure 4-2), where security and forwarding service times have been modelled explicitly by a 2-stages hypoexponential distribution in which the service rates are different [71]. The impact of business has not been taken into consideration. In addition, only single-class, which served according to FCFS discipline, was considered.

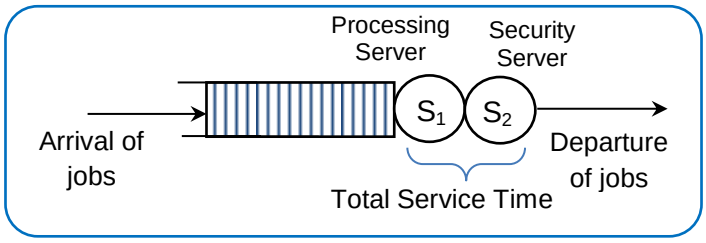


Figure 4-2 QN of a MANET node with two servers

The performance-related security modelling and evaluation of a static RANET node with a WEP security mechanism was also investigated in [64] through QNs. A MANET node was modelled as a queueing system with either single or dual server, where security was represented by a delay centre. Both inter-arrival times and service times follow GE distribution. In both models, mobility was not taken into consideration.

In order to make MANET/RANET's model more realistic, the concept of mobility modelling in MANETs / RANETs should be taken into consideration. Bhatia et al. [18 , 59] proposed a Gated Queue (G-Queue), where each node has an 'On-

Off' gate to reflect the presence/absence, respectively, of a link with another network node. The concept of modelling mobility in MANETs / RANETs in the literature is described in more detail below.

e) Mobility Modelling of MANETS / RANETs Using QNs

Since RANETs' functionality involves mobility, it is vital to model robotic nodes movements as well as the wireless links behaviour within the static queueing node, subject to the characterisation of the incoming traffic, and evaluate the network's performance-related security. Mobility is the main cause of the link breaking down as the connection between two RANET nodes becomes unavailable often because one of the nodes has moved out of the coverage area of other nodes [59].

Several approaches were suggested to model the channel availability within queueing nodes of a MANET, based on 'G-Queues', 'Server vacation' and 'Intermittent links'. These approaches use the IPP to capture the input/output link availability to/from a mobile node (c.f., [18 , 59 , 88 , 89]). This study will focus only on G-QN since they have been used in the proposed models for its simplicity. More information can be found on other models in [18 , 59 , 88 , 89].

i) G-Queues

RANET nodes can be modelled as a stable open G-QN model, where the wireless links between a pair of nodes are either available or unavailable through 'G-Queues' (c.f., [18]).A G-queue, depicted in Figure 4-3, is a gate introduced at the entry of QN model, which represents the input link to that node. This input link goes 'Off' and 'On' exponentially with mean rates of α and β, respectively. When the link is up, it is said to be in phase 'On' and when it is down it is in state 'Off' (i.e., the node is disconnected from the RANET).

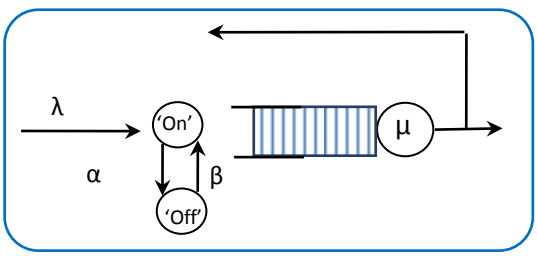


Figure 4-3 A RANET node with a gated queue (c.f., [18])

Note that the external mean arrival rate is denoted by λ whilst μ refers to the mean service rate.

f) ME

ME is an analytic tool used to determine" the probability distribution of the number of jobs in a queuing system by maximising the corresponding entropy" [90] subject to constraints in terms of mean number of jobs in the system. ME algorithm proposed in [20 , 74] can be applied in the context of performance versus security trade-off in high-speed networks modelled by for M router queues connected to form arbitrary open QN with and R priority classes, finite capacity with blocking, where the exact solution of such a network cannot often be performed (c.f., [16]. Thus, exploiting ME principle helps in overcoming potential state space explosion caused by increased the network size and the inclusion of multiple classes and blocking mechanisms. By applying ME, secure network can be decomposed into M individual queues with R classes, each of which can be approximately analysed in isolation to determine, in a cost-effective way with acceptable accuracy, the required aggregate and marginal performance metrics. These metrics then express the scales of improvements in performance in the secure systems.

4.3.2 PNs and Generalisations

In this section, fundamentals of PNs and their generalisations such as Stochastic PN (SPN) and GSPN models are described. In addition, two case studies from the literature on the use of these models in modelling and evaluating of the performance-security trade-off are presented.

a) Fundamentals of PN-based Models and Generalisations

PNs are credible modelling tools for the qualitative/quantitative analysis of complex system involving software contention, blocking and synchronisation. However, PNs and its generalisations cannot directly represent scheduling disciplines [82 , 83], motivating the use of extensions to increase their system-modelling capabilities and analyses (c.f., [91]).

i) PNs

A PN is a bipartite directed graph and it is composed of two types of nodes: 'Places', p, and 'Transitions', t. A place is plotted as a circle and accommodates customers called 'Tokens', the total number of which defines its state. Transitions, plotted as boxes or bars, represent events/actions that change the system's state. Arcs are the links between places and transitions representing interdependencies between them. Note that these arcs cannot be used to connect places to places or transitions to transitions. The marking (M) of the PN is known as the number of tokens in each place and M_0 indicates the initial marking of the PN (c.f.,[89 , 91 , 92 , 93]).The reachability set (or state space) can be defined as a group of markings reached from M_0 as a result of sequential firing of transitions. Thus, a state space for a PN can be either finite or infinite, according to PN structure. State space explosion may occur when there is a very large set of markings of the PNs (c.f., [89 , 91 , 92 , 93]). When an arc connects from a place to a transition, this place is known as 'Input place', whilst if an arc connects from a transition to a place, this place is known as 'Output place'. These concepts are depicted in Figure 4-4.

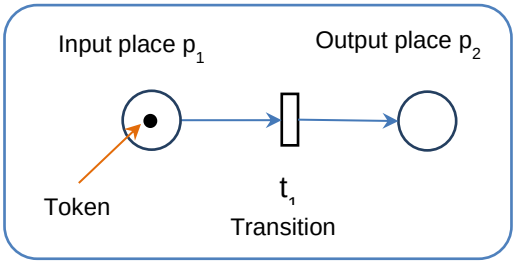


Figure 4-4 Typical components of a PN (c.f., [89 , 92])

A transition is considered to be enabled if the number of tokens in each of its input places is at least one. Once enabled, firing of a transition may possibly change the state of the system and, consequently, the number of tokens in each of the input places for that transition is reduced by one token or more (according to the input arc multiplicity, connecting from a place to a transition). Similarly, the number of tokens in each of its output places is increased by one

(or more according to the output arc multiplicity, connecting from a transition to a place).

Since time was not considered in traditional PNs, several extensions have been proposed to allow the performance analysis of more realistic systems to be evaluated. PNs can be extended by assigning time delays to places, transitions, arcs or tokens, and the resulting systems are known as Timed Petri Nets (TPNs). In these extensions, time was assumed to be either deterministic or stochastic (c.f.,[89 , 91 , 92 , 93]).

ii) SPNs

When this delay is exponentially distributed, the resulting Timed Transitions PNs (TTPNs) is referred to as a SPN. The firing policy adopted for an SPN is the 'Atomic firing policy' (c.f., [89]), according to which firing of a transition (after a random period of time) is considered as an 'Atomic' operation in the sense that tokens are removed from input places and deposited into output places with one indivisible action.

iii) GSPNs

Since SPN-based modelling and evaluation of complex networks may become increasingly time-consuming with the potential of a state explosion, a GSPN was introduced in [89] as an attempt to address this problem and execute immediate transitions and inhibitors, where the corresponding states vanish, as appropriate. These immediate transitions have priority of firing over the 'Timed' transitions. Another type of arc was also defined as 'Inhibitors', where the absence of tokens in an input place linked to this arc enables the transition for potential firing, given that the other input places have at least one token each (c.f., [89 , 91 , 92]).

Some of the GSPN limitations are inability to model scheduling strategies. Moreover, PNs and their extensions (c.f., [89 , 91 , 92 , 93]) suffer from state space explosion as the network size increases. This is due to the fact that a GSPN model has the ability of provide "compact representations" [94] of complex systems which is, in turn, reflected in the sizes of their state spaces

that grow with the number of places in GSPN and of tokens in its initial markings [94].In the context of this study, GSPN is utilised to model security mechanism in order to evaluate more effectively the adverse impact of security on performance and associated trade-offs.

b) PN-based Applications into Performance and Security Trade-offs

For illustration purposes, two key modelling applications on performance vs. security trade-offs in MANETs with Intrusion Detection System (IDS) using SPN [15]and a general communication system with encryption protocol using GSPN [13], are discussed below:

i) An SPN Model for Performance vs. IDS-based with Rekeying Security Trade-off for a MANET

*C*ho et al.[15] analysed an SPN model focusing on the assessment of group communication system (GCS) vs. IDS-based with rekeying for a MANET.

- *Model Description and Application Context*

Cho et al. [15] developed a robust SPN model for the evaluation of trade-offs associated with performance and security properties of a GCS for MANETs, which employs voting-based IDS with batch rekeying techniques in which a compromised node is evicted from the communicating group when the majority of nodes vote against it, and this is performed in a periodic manner at each node. Cho et al. [15] adopted a threshold-based periodic batch rekeying in order to reduce the rekeying overhead in MANETs attributed to the joining, leaving and evicting of nodes. The optimisation of this threshold value is important, since a large threshold value gives compromised nodes the opportunity to access data (i.e., violating security), whilst a low threshold value increases the computations and the rekeying overhead (i.e., degrading performance). The evaluation of the adopted SPN in [15] led to the identification of optimal settings in terms of batch rekeying intervals, maximise MTTSF and minimise mean response time simultaneously.

- *Performance and Security Metrics Considered*

SPN's model performance metrics are response time (R) and MTTSF (i.e., time between rekeying operations), as performance and security measures, respectively.

- *Remarks*

The SPN model of MANET in [15] was made at network level and not at the node level. Consequently, the characteristics of a single node might not be taken explicitly into consideration and this might prevents assuming the heterogeneity of nodes (i.e., it will not be easy to reflect the behaviours of various nodes in the proposed SPN).

ii) A GSPN Model for Performance vs. Encryption-based Security Trade-off for an Abstract Communication System

Wolter and Reinecke [13] proposed a GSPN model of an abstract communication system with encryption protocol, based on a CPSM to investigate the performance and security trade-offs.

- *Model Description and Application Context*

Wolter and Reinecke [13] proposed a combined performance-security model for an abstract communication system, based on a GSPN, in order to evaluate and optimise the trade-off between performance and security by means of a combined metric (c.f., Figure 4-5).

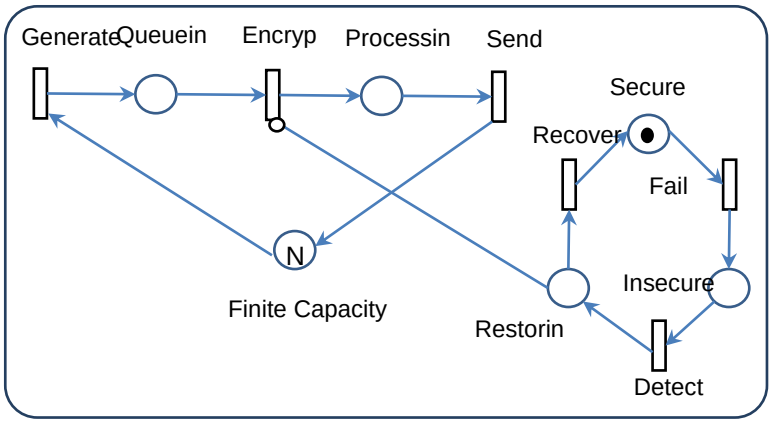


Figure 4-5 Wolter and Reinecke [13] model for a performance and security trade-off

The GSPN consists of two models, one for ‘Security’, modelling the encryption-based security state of the system (the encryption key in particular) and one for performance, representing encryption processing and transmission.
Once the encryption key is broken, the system becomes insecure and recovery process which requires producing a new key is performed. The two models are linked by an inhibitor arc, which connects the place ‘Restoring’ in the security model to the transition ‘Encrypt’ of the performance model.

From the encryption application point of view, the system will act as follows: when the system is secure it encrypts and transmits messages. Once the encryption key is broken, the system becomes insecure and, in this case, messages are encrypted by invalid key and this indicates the leakage of sensitive information. When the system detects this problem (which is usually related to the integrity test included in the encryption protocol), the encryption process is interrupted and it stops/is inhibited until a new key is generated. During the time between key being compromised and detecting this incident, any encrypted message with the broken key can be seen as unsecure (i.e., information leakage). The adverse effect of security on performance is accounted for in terms of the security processing and potential extra delays due to the presence of a token in the security system state ‘Restoring’ of the security model (due to the inhibitor arc), which blocks the encryption process. This model investigates how to choose an appropriate encryption key length in terms of its corresponding encryption time.

From one hand, the longer the encryption key, the higher the security level of encrypted messages which means they become more secure. On the other hand, longer key length increases the computational effort resulted by encryption. Thus an appropriate trade-off is needed.

- *Performance and Security Metrics Considered*

1. *Performance Metric*

The performance metrics considered is the ‘Throughput’ of ‘Send’ transition within the performance sub-model.

2. Security Metrics

Security metrics in this model were expressed in terms of probabilities of events to occur [13], e.g., ’Probability of the system being in secure state’; ‘Probability of the undetected broken key’ and ‘The probability of detected broken key’.

3. CPSMs

An ‘Optimal’ trade-off between security and performance was established in [13] by proposing CPSM to determine an optimal key length for the encryption process that corresponds to the CPSM maximum value. CPSM is defined as *“the sum of th*e throughput *of the performance model and the probability of the system being in the ‘secure’ state (or, place) in the security model”*, i.e., (throughput of performance sub-model) + (Probably of the system to be secure e.g., P (Secure), as depicted in Figure 4-6.

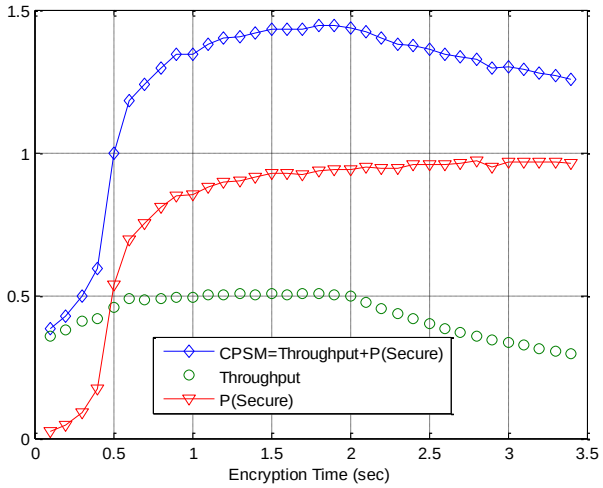


Figure 4-6 CPSM proposed by Wolter and Reinecke (adapted from [13])

The optimum encryption time is 2 sec and it means that when using the corresponding encryption key length, both performance and security are maximise and using longer encryption keys causes performance degradation in spite of improving security. Wolter and Reinecke[13] state that CPSM gives a measure that comprises the contribution made by performance besides security

and it should have a maximum. It is noteworthy that the throughput obtained in the model has a maximum since the capacity of the system is limited.

- *Remarks*

Wolter security model does not take bursty traffic into consideration. Appropriate extensions can be made to security sub-model in order to express more sophisticated scenarios for security protocols and control to provide, for example, the protection against information leakage. In order to make the CPSM more appropriate, utilisation can be used instead of the throughput since the latter is considerably greater than unity in context of high-speed networks and therefore; it will dominant the overall CPSM (after being added to the appropriate probability). Utilisation, on the other hand, is a fraction thus it has the same scale as probability does. Moreover, both utilisation and probability values are dimensionless.

4.3.3 Combined QNs and GSPNs

Due to the limitation of QNs and GSPNs, several suggestions have been made in the literature to combine them in one model in various forms (c.f., [80 , 82 , 83 , 89 , 95 , 96 , 97 , 98 , 99]).This combination can be generally classified into two main types of modelling tools involving integrations of GSPNs and QNs, namely:

1. *Embedding a QN in a PN Component* (c.f., [82 , 83 , 95 , 100]);
2. *Integrating/Combining a QN with a GSPN*(c.f., [80 , 82 , 83 , 89 , 95 , 96 , 97 , 98 , 99]).

This section will focus on the second type of combination between QN and GSPN, i.e. integrating QNs with GSPNs; it will then review one of the combination approaches which investigate the trade-off modelling between performance and reliability.

a) Fundamentals of Combined QN and GSPN Models

QNs and GSPNs were combined in order to exploit the best features of both modelling tools to overcome their limitations and provide an effective analytic solution to complex systems by including the required level of detail in the

model [86]. The concept of combining GSPNs and QNs was introduced for the first time in the literature by Balbo et al. [86] where he presented two case studies as example on the use of combined QN and GSPN model. In his first case study, for example, Balbo et al. modelled concurrency and synchronisation of software task executions on a system with M servers (CPU's, I/O units). At modelling level, concurrent execution of tasks in software part were modelled by GSPN where the CPU and I/O units by Product Form Queueing Networks (PFQN) model. While at analysis level, QN part of the model was converted to a single timed transition using Principle of Flow Equivalence' (FE) in order to reduces the state space of the underlying Markov chain of the overall GSPN model (c.f., [86 , 101] .However, Balbo et al does not provide a general and clear combination structure that can facilitate modelling of other various problems (c.f., [80 , 96]). Moreover, the performance and/or security of the proposed model were not evaluated.

While in [97], Szczerbicka exploited the same combination approach to model the performance and reliability of a fault-tolerant computer system, which will be described in more detail in the next section. At modelling level, GSPN represents the 'Fault model' of the transmission channel fault and correction while QN model reflects the performance of the system. At analysis level, similarly to Balbo approach, Szczerbicka suggested the replacement of QN with either an equivalent timed transition or more complex GSPN-structure in order to eliminate the state space explosion of GSPNs.

In a different context, Becker and Szczerbicka [80] proposed a Petri Nets including Queuing networks (PNiQ) to model and analysis manufacturing schemes, where a single-class QN was combined with a GSPN, in which QNs reflect the manufacturing production lines, while GSPNs captures the associated control and maintenance process. This model is then extended to Multi Class-Petri Nets including Queuing networks (MC-PNiQ) [96] model to count for multiple classes which was solved analytically using the flow-

equivalent concept, and this leads to a very large percentage reduction of state space from 50% to 95%.

As adifferent analysis approach, Szczerbicka and Ziegler [102] devised a simulation-framework based on active objects for the combination of a GSPN and QN as quantitative tool for evaluating the performance and reliability of computer systems, taking advantages of common abstract features between QNs and GSPNs (i.e., both transitions and servers represents events where the queue buffers and places represents a node condition).

b) Advantages of combining QNs and GSPNs

1. Combining & exploiting the *best features* of both QNs and GSPNs to provide an effective & "computationally manageable" [102] solution of dynamics, control and security of a system analytically or via simulation (c.f., [102]) and acting as a general purpose technique for solving certain classes of "Non-product form models" (c.f., [80 , 86 , 97]);
2. Reducing the *state space explosion* and the model 'graphical complexity'[96] where hardware interactions, routings, multiple classes & blocking can be modelled by QNs while software operations e.g., synchronisation and concurrency are reflected by GSPN (c.f., [80 , 86 , 97]);
3. In the context of DES, adopting combined QNs & GSPNs will help in reducing the time required to update transitions status after each firing event in a pure GSPN model (as the overall number of transitions/places required to model the same system is reduces).

c) Combined QN and GSPN-based Applications to Performance and Security Trade-offs

Security was not considered straightforward in this study as reliability was investigated instead [97]. In particular, a combined QN and GSPN model was used to reflect the performance and reliability trade-off of a fault-tolerant computer system, (c.f., Figure 4-7), consisting of a central processor working according to processor sharing mode, with two local I/O units besides a remote one connected to the system through a communication channel. The reliability

of this channel was modelled by a GSPN whereas the processor and its local units were modelled by a QN [97].Transmissions (with the rate λ_{send}) to/from the remote unit can be interrupted when the channel fails. Consequently, all transmitted jobs and those waiting for transmission are performed again in the CPU and they form a Poisson process with parameter λ_{pert}. For higher failure rates, the system's throughput decrease since it cannot cope with the increasing number of returned jobs due to its limited processing power. The study then investigated the trade-off between CPU processing rate and channel failure rate. The combination structure is only customised to this particular application. Moreover, the pure metric 'throughput' was used to investigate the trade-off between the system's performance and channel's reliability for single class and non-bursty traffic within infrastructure network.

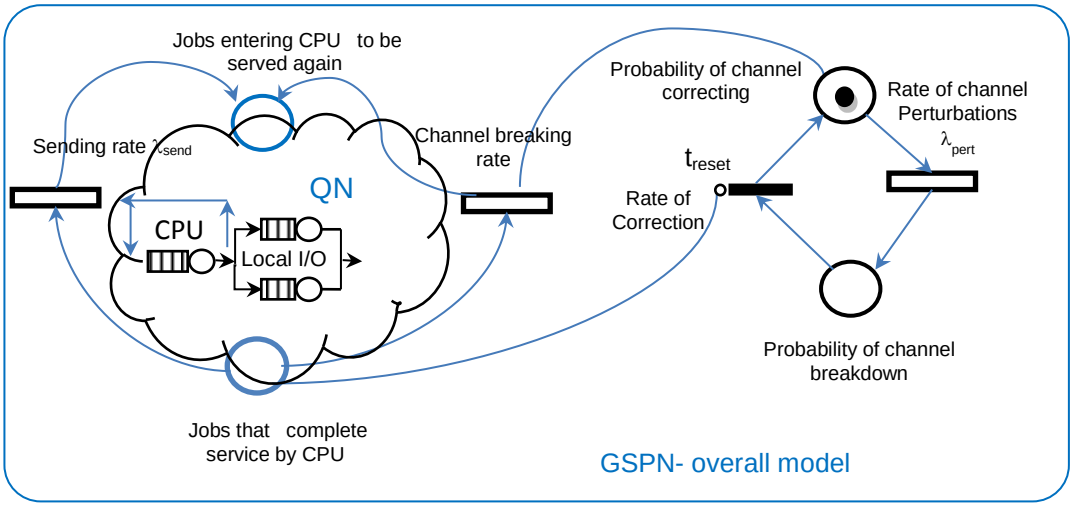


Figure 4-7 The Combined QN and GSPN proposed by Sczerbicka (c.f.,[97])

- *Remarks*

It is worth mentioning that the suggested modelling approaches (i.e., [80 , 86 , 96 , 97 , 99]), were used to perform modelling at the system/network level, however, they have not been used at nodal-level. In addition, the focus was mainly on reducing the state explosion when a single class is used. The proposed combined models were also customised to particular application thus they can hardly been generalised to reflect other various applications. These studies also presented analytic solutions and the performance and security evaluation were not considered except in Sczerbicka's model which

investigated the performance- reliability trade-offs and it was associated only with the throughput as a main metric.

Combined QNs and GSPN modelling approach can be beneficial in the context of RANETs where the security operations (i.e., software part) can be reflected by GSPN model while the data processing (i.e., the hardware part) can be simply modelled using a QN model.

To the best of the researcher's knowledge, this modelling approach has not been made in the literature in the context of performance and security trade-off in infrastructure communication networks. It was either applied in the context of computer science and manufacturing applications [80 , 86 , 96 , 99]), or the performability of a distributed systems [97].

Finally, performance-security evaluation of trade-offs in RANETs requires not only the adoption of appropriate quantitative modelling tools but also the joint optimisation of CPSMs. Thus combined QN and GSPN modelling approach can be used together with appropriate CPSMs.

3.4 Summary

This chapter reviewed the quantitative modelling and evaluation tools of performance and security trade-offs which are QNs and GSPNs models. It also described some existing case studies to model and evaluates the trade-off using QNs and GSPNs. Finally, the concept of CPSM was described as a new measure to simultaneously optimise performance and security. In the following chapter, the proposed QN models for investigating the trade-off between performance and security in routers will be presented.

Chapter 5 Modelling Performance and Security Trade-off for Routers in High-Speed Networks Using QNs

5.1 Introduction

One of the key components affecting the performance of infrastructural high-speed networks in the realm of today's voluminous traffic is the router node. The router is expected to process incoming messages with minimum delay and high-speed, subject to security constraints; however, the activation of the ACL security option in routers consumes the router's CPU usage is which causes its performance to deteriorate [3 , 5]. Moreover, the gap between the router's CPU processing power and the high-speed incoming traffic may cause a bottleneck in the network and this considerably affects the overall performance of the network. Consequently, packets processing is considerable delayed which causes performance deterioration of the overall high-speed network.

It is vital to establish a feasible level for the router's performance degradation and to determine whether this is acceptable for real-time applications. To quantify and predict the trade-off of this degradation, a quantitative analysis methodology is employs an appropriate QN model to predict and improve the performance of the secure router under heavy traffic conditions. This chapter has carried out, through DES, an investigation into the negative impact of the ACL security application on the router's performance. It also considers the security modelling of the Extended-Inbound ACL function within high-speed router both implicitly and explicitly using two different QN models. Implicit modelling of security is performed by decreasing the service rate (forwarding rate) of the router's CPU by a predefined percentage, while the explicit modelling is achieved by assigning an individual QN node representing Extended-Inbound ACL security function, which is connected in tandem with another QN node presenting the forwarding queue.

Both QN models have single-core and quad-core processors for FCFS and HoL subject to CBS and PBS buffer management schemes. Service priority and space priority are suggested as an attempt to adopt Performance-engineering concepts to reach a performance-related security trade-off in high-speed networks. Both inter-arrival and service time distributions are modelled by the GE, which is completely defined in terms of its first two moments [12], in order to reflect the inter-arrival times of packet traffic burstiness and the variability of service times at the router node. Numerical experiments and comparative studies of performance versus security under typical scenarios are presented. The considered metrics for both models are the router's mean response time, packet loss probability.

As a future research direction, an analytic methodology is explored, based on the principle of ME, for the cost-effective performance related security modelling and evaluation of high-speed networks using arbitrary open queueing networks (QNs) models with finite capacity[20], [16].

5.2 The Router and the ACL Security Mechanism

Performance of the router is adversely affected by ACL activation since the router needs to perform more computations [3 , 39 , 49]. In the following section, a QN model is proposed to evaluate and predict the router performance in the presence of security. Note that the Extended ACL is selected in this study since it requires longer time to match several criteria during traffic filtration. In addition, inbounded ACL, in which traffic filtering is applied for a packet before it is processed for routing [48], is considered in this study.

5.3 The Proposed Models for the High-Speed Router

In this section, a QN model is proposed for a high-speed router with ACL security mechanism. The computations impact of ACL on the router performance is modelled in two ways:

- **Implicitly**, where the service rate of the router's CPU (or server) is reduced by a small percentage, p;

- **Explicitly**, where the security is modelled by a separate QN node. This approach is similar to the one suggested by Saleh and Alkhatib[14 , 103].

The two ways besides the proposed QNs are described as follows.

5.3.1 Modelling Security Implicitly

ACL mechanism's action within a high-speed router is modelled implicitly by using a single finite capacity queueing model with GE inter-arrival and service times distributions. This approach is similar to the one proposed by Zorkadis [6] to model security using QNs. However, the Zorkadis assumes a less values for the service rate instead of defining a reduction rate. The proposed models for the router subject to FCFS and HoL disciplines are shown in Figure 5-1 and Figure 5-2 respectively.

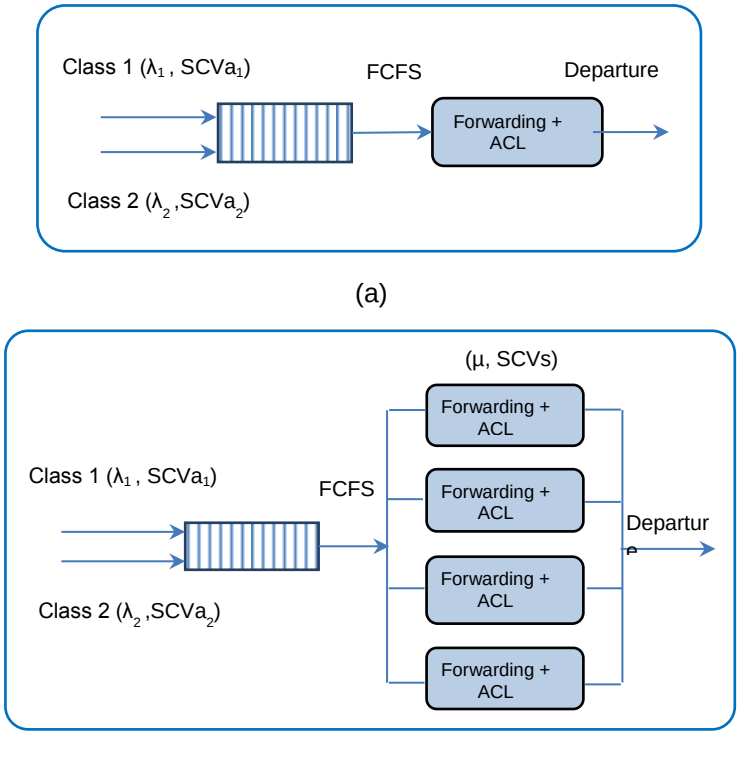
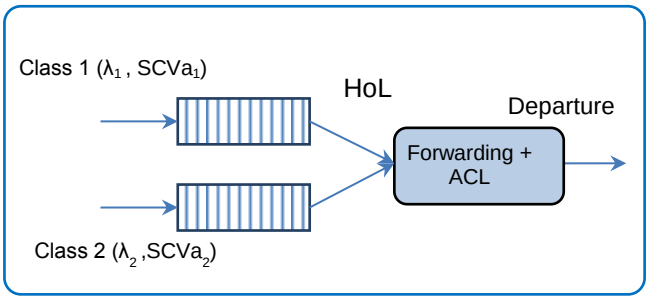
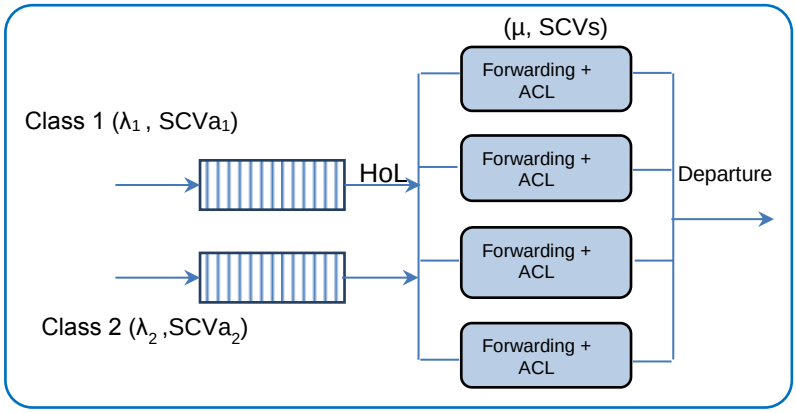


Figure 5-1 The proposed QN models of the router with FCFS discipline (a) single-core CPU router, (b) quad-core CPU router



(a)



(b)

Figure 5-2The proposed QN models of the router with HoL discipline (a) single-core CPU router, (b) quad-core CPU router

a) The Performance Metrics

The performance metrics of this study give a clear idea of the router's performance-related security functions, showing how fast and reliable it is; they are as follows:

1. Mean Response time (W)

   This is the time taken by a router to process a packet (i.e. the time between receiving data and forwarding data out of the router). It differs according to the queueing discipline used [104].

2. Packet Loss Probability (PLP)

   This is the percentage of packets that get blocked / lost on arrival if the router node is at full capacity [104].

These performance metrics were chosen because they are directly affected when the router is overloaded in the event of congestion. Any significant increase in these values may lead to the assumption that congesting has occu-

rred, which may be a symptom (result) of an attacks.

b) Simulation Input Description

DES [105] code was implemented using a Java package to simulate GE/GE/c/N/FCFS CBS, PBS and GE/GE/c/N/HoL CBS in terms of router response time and packet loss. The program was run up to 15 independent times. GE distribution is considered a limited case of hyperexponential distribution (H_2) with high value of the tuning parameter K (K approaches infinity), as stated in [106]. Table 5-1 shows sample experimental results (together with 95% confidence intervals).

Table 5-1 Simulation results for the secure high-speed router

λ_1	Packet Loss	95% CI	*Mean Response Time*	95% CI	Aggregate Utilisation	95% CI
1×10^5	0.0029	±0.0001	2.791×10^{-6}	$\pm27\times10^{-9}$	0.239	±0.001
2×10^5	0.0053	±0.0002	3.556×10^{-6}	$\pm31\times10^{-9}$	0.299	±0.002
3×10^5	0.0090	±0.0003	4.435×10^{-6}	$\pm30\times10^{-9}$	0.357	±0.001
4×10^5	0.0148	±0.0002	5.427×10^{-6}	$\pm36\times10^{-9}$	0.415	±0.001
5×10^5	0.0220	±0.0005	6.400×10^{-6}	$\pm38\times10^{-9}$	0.469	±0.001
6×10^5	0.0325	±0.0007	7.521×10^{-6}	$\pm53\times10^{-9}$	0.522	±0.002

Single-core and quad-core CPU performance was firstly compared for both FCFS and HoL disciplines to show that quad-core outperforms single-core. Then the quad-core CPU router model was simulated without considering the security component, after which the security effect on forwarding speed was taken into account.

The main aim is to assess the adverse effect of the security mechanism on the performance of the router and check the performance gain when a quad-core processor is used under FCFS and HoL service disciplines. In this context, two priority classes are considered, namely video conversation and file transfer. The first class requires high bandwidth and is sensitive to the router delay as it is a real-time application. The simulation input values are as follows:

Mean arrival rate λ_1 was in the range 1×10^5 to 6×10^5 packets/sec for the high-priority class and $\lambda_2 = 3\times 10^5$ packets per second for the low-priority class. SCV for the inter-arrival times are SCV_{a1}= 4, 8 and SCV_{a2} = 4, 8. Mean service rate

$\mu = 4.16 \times 10^5$ packets /sec and SCVs= 4.The simulation program was executed for both CBS and PBS. The threshold for the PBS was set to 10% and 30% which means that when low-priority class packets occupy 10% (or 30%) of the buffer space, not further packets of this class are allowed to enter the queue.

The number of CPU cores = 1, 4 (i.e., single-core and quad–core processor respectively). The buffer size was 50 packets for both FCFS and HoL and the choice of such a low value was justified in [106] for high-speed routers. The packet size is assumed to be 1500 bytes (as in Ethernet [4]), so the total bandwidth for both classes is 5 Gbps (given that the router forwarding rate is 5Gbps and, in terms of packets per sec, it is 5Gbps/ (1500 ×8) =0.416 MBps) and the total input load is in the range 4×10^5 to 10.16×10^5; i.e., the maximum applied load is twice that of the router's forwarding speed.

As stated in [3], the security component ACL has a massive effect on the router forwarding speed and it represents a bottleneck for routers in high-speed networks. In the simulation, the security degradation effect parameter [6] was defined and assumed to degrade the router service rate by 15%, for illustration purposes. These two values were expressed as follows:

```
Security_degredation=0.15;
Forwarding_Speed=1-Security_degredation;
Mean_service_rate= Forwarding Speed*V2;
```

where V_2 is the router mean service rate.

c) Results

Results shown from Figure 5-3 to Figure 5-6 show the relations between the adopted performance metrics for the router node as functions of the high-priority class mean arrival rate in order to check the bursty effect on such a class, which requires the best service by the router, and also to study its impact on the low-priority class. The effect of buffer-sharing methods was also taken into account by the simulation. Four different scenarios were applied for the queueing models. Table 5-2 summaries these scenarios.

Table 5-2 Simulation scenarios

Scenario	Criteria	Description
A	C=1,4; Sec='Off' FCFS, HoL; SCVa1=SCVa2= 4.	Effect of the number of cores in the router CPU on the performance.
B	C=4, Sec='On', 'Off', FCFS-CBS, HoL-CBS.	Comparing between FCFS and HoL with and without security activation.
C	C= 4; Sec='On', 'Off'; SCVa1=SCVa2=4, 8;	Assessing the effect of SCV of the packets inter-arrival on the performance.
D	FCFS-CBS, Sec='Off', FCFS-PBS, Th =10%, Th = 30%, Sec='On'.	Assessing the threshold value effect on the router performance

i) Effect of the Number of Cores in the Router CPU on the Performance.

Figure 5-3 illustrates the comparison of the single-core and quad-core CPU and the effect of the core number on the router performance in terms of router's CPU packet loss probability, when security application is 'Off' where the performance of the router is not affected by security. It is obvious that the use of quad-core CPU considerably reduce the router's packet loss probability.

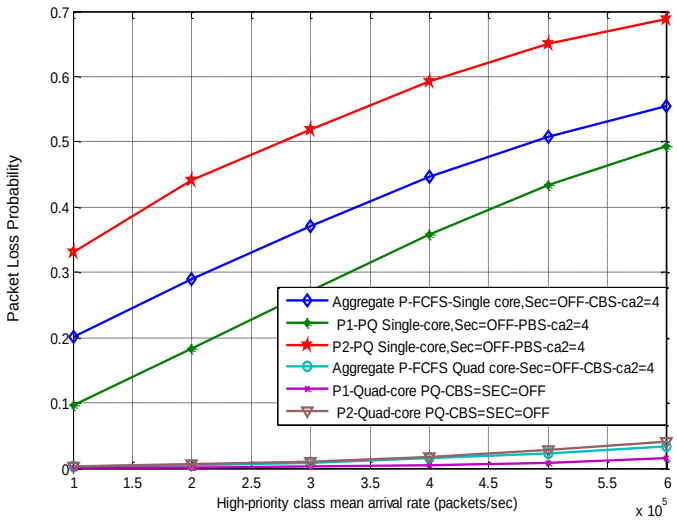


Figure 5-3 Router PLP for single-core and quad-core CPU for FCFS and HoL disciplines with security 'On'/'Off' for λ_2= 3× 10^5 packets /sec

ii) Effect of the Security Component on the Router Performance

Figure 5-4 shows the comparison between the simulated service disciplines in terms of PLP for the quad-core CPU for security 'On' and 'Off' for $\lambda_2 = 3\times10^5$ packets /sec. It is clear that the presence of the ACL mechanism degrades both queueing systems. The HoL model gives, as expected, better trade-off between

performance and security for high-priority packets in terms of PLP, Since HoL high-priority classes have the lowest packet loss, and they are served first by the router. The low-priority class packet loss is discriminated here. The packet loss increased once the security was activated since the router buffer overflowed faster, and any incoming packets were discarded, as no space was available.

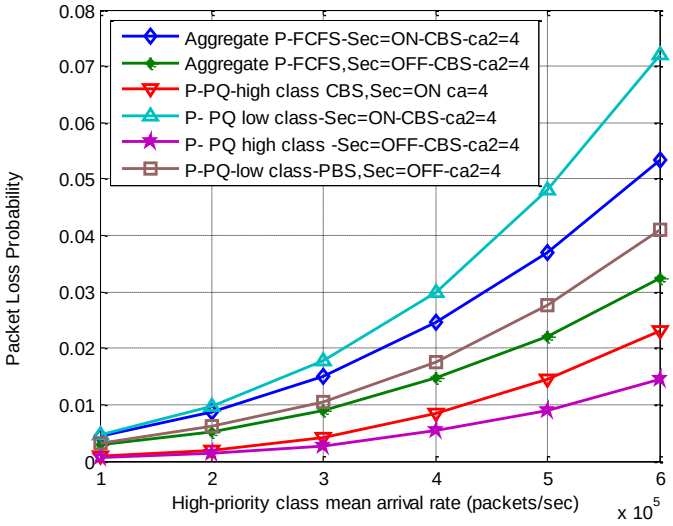


Figure 5-4 Router PLP for quad-core CPU FCFS and HoL disciplines with security 'On'/'Off' for λ_2= 3× 10^5 packets /sec

iii) Effect of Traffic Burstiness Degree on the Performance of the Router

The increase in the burstiness of the arrival process of packets degrades the system performance during the activation of the ACL mechanism. Figure 5-5 depicts the behaviour of the router when the traffic burstiness of the arriving packets is increased. It is clear that the performance is worsening. In fact, since the current applications require data to be transferred at high-speed, the router should forward these data coming from difference sources and at different speeds, at an acceptable speed compared with its standard forwarding power. It is important to make the router secure at all times, since most of today's applications require access control provided by the router. Therefore, combining the effect of ACL activation and the high data burstiness should be taken into consideration. In terms of the router's PLP, it is obvious from Figure 5-5 that the router's performance deteriorates (i.e., marginal as well as aggregate PLP

becomes higher). It is obvious that the use of HoL discipline discriminates low-priority class packets and PLP which is further degraded by increasing burstiness of high-priority classes.

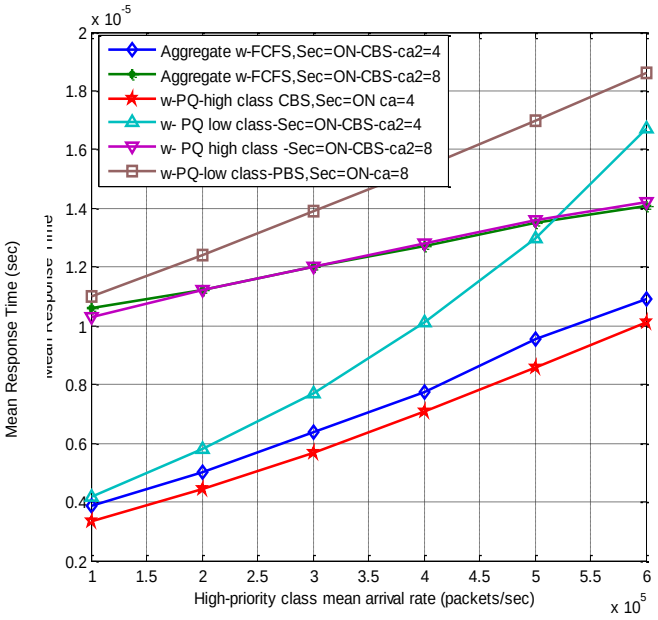


Figure 5-5 Router mean response time comparison for quad-core CPU for FCFS and HoL discipline with security 'On'/'Off' for λ_2=3× 10^5 packets /sec and Ca^2 = 4 and 8

iv) Effect of Buffer-Sharing Schemes on the Router Performance

The CBS and the PBS buffer management schemes are implemented under the FCFS service discipline. It is assumed that arrivals occur with mean arrival rate λ_1 as class 1 and mean arrival rate λ_2 as class 2.

Figure 5-6 shows the comparisons between the router's mean response time for FCFS under CBS and PBS with and without security activation. The router performs well in the BPS in general and its performance is gradually improved with the decreasing of the threshold value. When the threshold = 10 %, the FCFS performs extremely well compared with the case of CBS in the presence of ACL mechanism. This is because the number of class 2 packets is limited to just 10% in the buffer of the router node. This gives class 1 packets a better chance of entering the router. In this case, class 2 packets are discriminated. The packet loss increased once the security was activated since the router buffer overflowed faster and any incoming packets were discarded as no space was available.

This indicates that PBS gives a good trade-off between performance and security in high-speed network routers. This holds even for a highly bursty traffic of arriving packets (by letting $Ca^2 = 8$). In fact, this improvement takes place on the cost of class 2 discrimination. Therefore, depending on the application nature of each class, performance Engineers can choose to discriminate the application that is less sensitive to delay and packet loss and with shorter packets (where variable packet sizes are mostly applicable). In this way, the most important application will perform at the required Quality of Service (QoS).

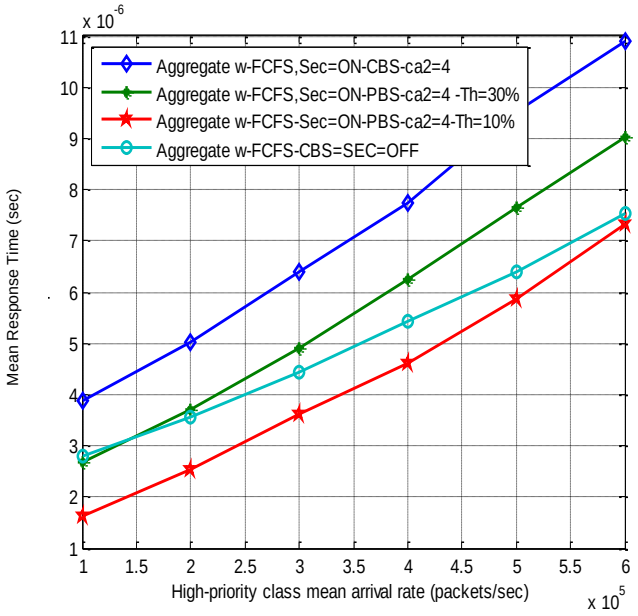


Figure 5-6 Router Mean response time for quad-core CPU-FCFS CBS and PBS discipline with security 'On'/'Off' for $\lambda_2 = 3 \times 10^5$ packets /sec

5.3.2 Modelling Security Explicitly

In this section, a more detailed queueing model for the router is proposed in which the ACL mechanism-denying function is taken explicitly into consideration.

Explicit security modelling was proposed by Saleh and Alkhatib in [14 , 103] where the security impact on performance was modelled as an extra service delay (i.e. a delay centre), which can be seen as one phase among hypoexponential distribution and jobs arrived according to FCFS discipline.

In this thesis, an explicit QN model is devised to represent ACL security mechanism. The performance of the router, in the presence of security, is then

evaluated by employing two GE-type queues in tandem with finite capacity and single-core and quad-core processors, as appropriate, to represent a router under FCFS and HoL service disciplines. More specifically, Extended-Inbound ACL security mechanism is represented as an explicit (independent) single server QN model which is connected in tandem with another QN model that reflects the processing function within the router which can be either single or quad-core CPUs. The router is assumed to have finite capacity queue with RS-FD blocking mechanism, to reflect ACL behaviour, subject to CBS and PBS management schemes. The arrived packets to the router are assumed to have two different classes which can be served subject to FCFS and HoL. DES is used to evaluate the performance degradation in terms of packet mean response time and PLP**.**

a) The Proposed QN for the High-Speed Router with ACL

This section introduces, in Figure 5-7 to Figure 5-10, four different scenarios of two queueing nodes in tandem, representing an ACL-related node 1 and an engine forwarding-related node 2 of a router with finite capacity, N, and two distinct classes of packets (c.f., R = 2). The order of queueing nodes is made since Inbound ACL is considered where security mechanism is applied first on the incoming packets then they can be processed and forwarded. The 'Accept-Deny' behaviour of ACL is explicitly reflected by RS-FD blocking mechanism.

b) Definitions and Notations

For each queueing node i, i = 1, 2 and packet class j, j = 1, 2, let:

λ_{ij} be the mean arrival rate of class j packets at node i;

C_{aij}^2 be the SCV of the inter-arrival time of class j packets to node i;

μ_{ij} be the mean transmission (service) rate for class j packets at node i;

C_{sij}^2 be the SCV of the transmission time for class j at node i;

ρ_{ij} be the server utilisation of class j packets at node i;

λ_{dij} be the mean inter-departure rate of class j packets at node i;

C_{dij}^2 be the SCV of the inter-departure time of class j packets at node i;

‘p’ be the packet acceptance probability by the ACL security mechanism thus ‘1-p’ representing the denying probability, and

‘θ’ be the threshold value for PBS scheme.

c) Description of Two Queueing Nodes in Tandem

In this study, the ACL and forwarding engine queueing nodes represent a router with or without ACL security mechanism, respectively, and they are modelled by either single-core CPU GE/GE/1/N/FCFS/CBS and GE/GE/1/N/HoL/CBS or PBS queues (c.f., Figure 5-7 and Figure 5-8 and) or quad-core GE/GE/c/N/ FCFS/CBS and GE/GE/c/N/HoL/CBS or PBS queues, respectively (c.f., Figure 5-9 and Figure 5-10).

Note that these queueing models can also be applied for firewalls, since they work in a similar way to the routers (when the encryption function is not taken into account in both the router and firewall).

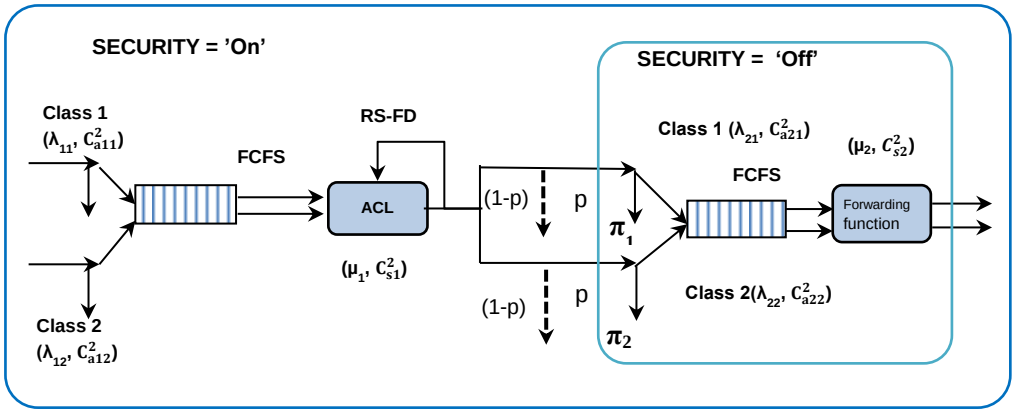


Figure 5-7 The queueing model for the router with single-core CPU and FCFS discipline

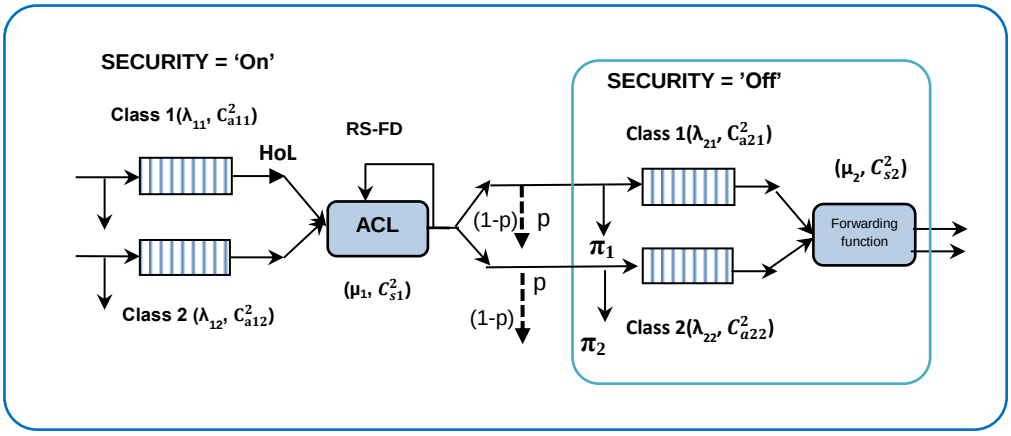


Figure 5-8 The queueing model for the router with single-core CPU and HoL discipline

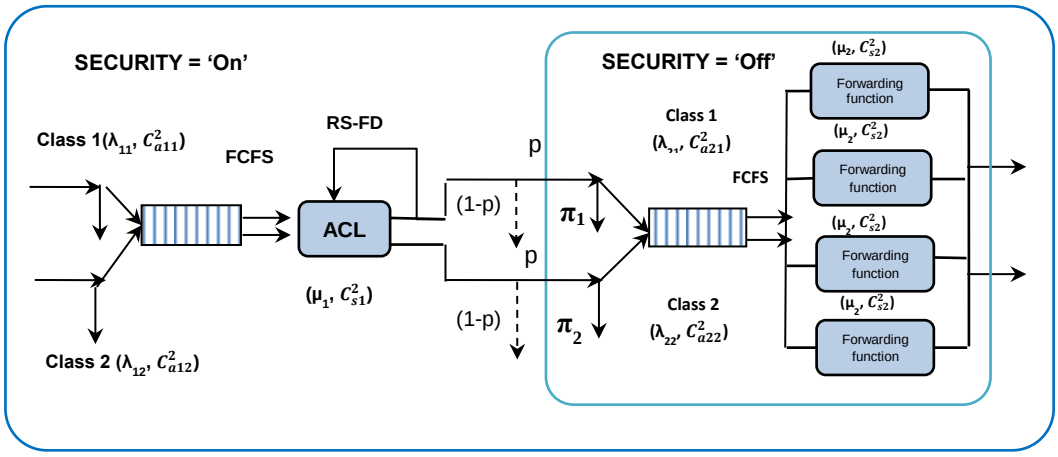


Figure 5-9 The queueing model for the router with quad-core CPU and FCFS discipline

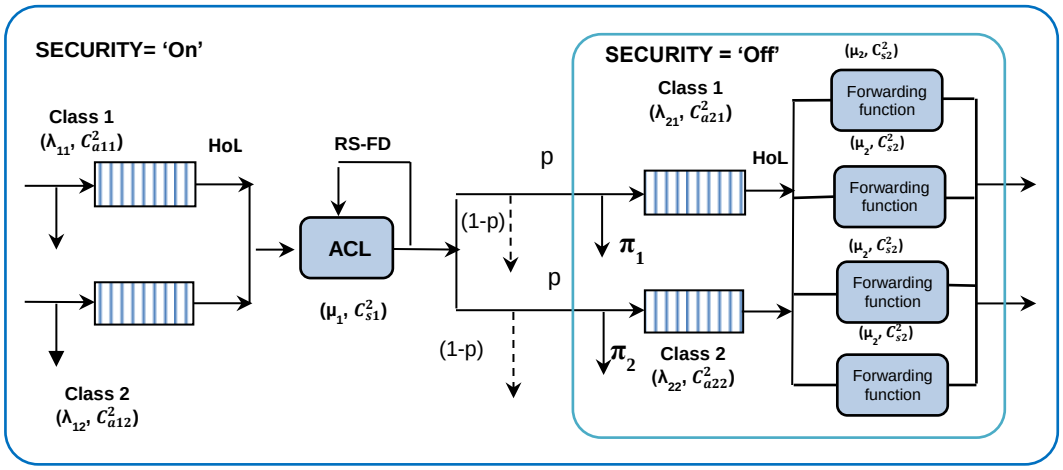


Figure 5-10 The queueing model for the router with quad-core CPU and HoL discipline

When the packet arrives at the router, it is assessed first by the ACL security mechanism at node 1. If the ACL node is full, the packet will be lost. Otherwise, upon service completion, this packet is either rejected with probability 1-p or accepted for transmission by the router with probability p. If the accepted packet finds the queue of the downstream node 2 with the engine forwarding function at full capacity, it will be blocked according to an adopted blocking mechanism (BM). For example, let the BM of the queueing model be represented by the Repetitive Service Blocking with Fixed Destination (RS-FD) in operation (c.f., [16]). Then the blocked packet immediately receives another 'Service' by ACL security node. This process is repeated until the packet completes its service at the ACL-related node at the moment when the forwarding queueing node 2 is not at full capacity. RS-FD has been selected over Repetitive Service Blocking with Random Destination (RS-RD) due to the nature of ACL mechanism, which

implies that the same packet should be treated in the same way by ACL (i.e., an accepted packet cannot be denied if it has been accepted by ACL).

d) Performance Metrics

Since the router's node is assumed to have two types of packets, performance metrics per class, which known as a 'Marginal metric', instead of the overall performance metric known as 'Aggregate metric', are considered '[34].

In this context, two performance metrics are adopted and are briefly described below:

1. *Marginal Mean Response Time (W)*

This is the mean time a router takes to process a packet of a particular class type (i.e., it is the mean time between receiving a data packet of a class at ACL queue (i.e., node 1) and transmitting it out from the forwarding function queue (i.e., node 2) of the router. This metric differs according to the queueing discipline used (c.f., [84], [2]).

2. *Marginal Packet loss Probability (π)*

This is the percentage of packets belong to a particular class type get blocked on departure from the ACL queue (c.f., node 1) if the forwarding function queue (c.f., node 2) is at full buffer capacity (c.f.,[2]).

e) Simulation Analysis

DES algorithm, based on the one described in [105], was implemented using a Java package to simulate the behaviour of the GE/GE/c/N/FCFS/PBS and GE/GE/c/N/HoL/CBS queues (with 95% confidence interval) in terms of the marginal mean response time and PLP at the router. The main aims of the simulation experiments are to assess the adverse effect of the ACL security mechanism on the performance of the router and predict the performance gain when a quad-core processor is used under FCFS and HoL service disciplines.

The program was run independently up to 60 times, using the GE-type distribution as a limited case of hyperexponential distribution (H_2) with a tuning parameter $k \rightarrow \infty$ (c.f., [12]). Single-core and quad-core CPU performance metrics were firstly simulated and compared under both FCFS and HoL

disciplines to assess the performance gains of quad-core CPU vs. single-core CPU with or without the application of the ACL security component of the router. For the HoL discipline, two priority classes are taken into consideration. The first class is assumed to be sensitive to the router delay and in need of high bandwidth. Four different scenarios and parameterisations for the queueing models employing single-core and quad-core CPUs, as appropriate, are summarised in Table 5-3.

Table 5-3 Simulation scenarios

Scenario	Router Topology and Parameterisation	Experiment
1	**Input Data:** c = 1; c = 4; FCFS-CBS; SEC = 'Off', 'On'; $\lambda_1 \in (10^5, 3 \times 10^5)$, $\lambda_2 = 10^5$; $SCV_{a1} = SCV_{a2} = 4$; $\mu_1 = 1.5 \times 10^5$, $\mu_2 = 10^5$; $SCV_{S1} = 8$, $SCV_{S2} = 4$; N=10. **Output Metrics:** Class 1 Marginal Mean Response Times, R_1 at the router.	Assessing the effect of the number of cores of the CPU with FCFS-CBS on the performance of the router for buffer size N = 10 with and without security activation.
2	**Input Data:** c = 1; c = 4; HoL-PBS; θ = 30%; SEC = 'Off', 'On'; $\lambda_1 \in (10^5, 3 \times 10^5)$, $\lambda_2 = 10^5$; $SCV_{a1} = SCV_{a2} = 4$; $\mu_1 = 1.5 \times 10^5$, $\mu_2 = 10^5$; $SCV_{S1} = 8$, $SCV_{S2} = 4$; N= 30. **Output Metrics:** Class Marginal PLPsπ_i, i = 1, 2) at the forwarding queueing node of the router.	Assessing the effect of the number of cores in CPU with HoL-PBS on the performance of the router for buffer size N = 30 with and without security activation.
3	**Input Data:** c = 1; c = 4; FCFS-CBS; HoL-PBS; θ = 30%; SEC ='Off', 'On'; $\lambda_1 \in (10^5, 3 \times 10^5)$, $\lambda_2 = 10^5$; $SCV_{a1} = SCV_{a2} = 4$; $\mu_1 = 1.5 \times 10^5$, $\mu_2 = 10^5$; $SCV_{S1} = 8$, $SCV_{S2} = 4$; $SCV_{a1} = SCV_{a2} = 4$; N=10. **Output Metrics:** Class1 Marginal total Mean Response Time, R_1 at the router.	Comparing the performance of FCFS - CBS vs. HoL-PBS for class 1 at the router for buffer size N = 10 with and without security activation.
4	**Input Data:** c = 1; c = 4; FCFS-CBS, HoL-PBS; θ = 30%; SEC ='Off', 'On'; $\lambda_1 \in (10^5, 3 \times 10^5)$, $\lambda_2 = 10^5$; $SCV_{a1} = SCV_{a2} = 4$; $\mu_1 = 1.5 \times 10^5$, $\mu_2 = 10^5$; $SCV_{S1} = 8$, $SCV_{S2} = 4$; $SCV_{a1} = SCV_{a2} = 4$; 'On'; N=30. **Output Metrics:** Class 2 Marginal PLP, π_2 at the forwarding queueing node at the router.	Comparing the performance of FCFS - CBS vs. HoL-PBS for class 2 at the router's forwarding queueing node for buffer size N = 30 with and without security activation.

The typical simulation input values of the scenarios are as follows: Mean arrival rate λ_1 in the range 1×10^5 to 3×10^5 packets/sec for the high-priority class and $\lambda_2 = 1 \times 10^5$ packets/sec for the low-priority class. The SCV for the inter-arrival times SCV_{a1} and SCV_{a2} are set equal to 4. The values of the mean rate and SCV for the service times are given by $\mu_1 = 1.5 \times 10^5$ packets /sec and $SCV_{S1} = 8$ for class 1 and $\mu_2 = 1 \times 10^5$ packets /sec and $SCV_{S2} = 4$ respectively. For class 2, the simulation program was executed for both FCFS and HoL under CBS and PBS, respectively. For illustration purposes, the threshold, $\theta = \theta_2$ for the PBS is set to 30% whilst the ACL denying probability, p, was set to 10%. The buffer size, N, is fixed to either 10 or 30 packets under both FCFS and HoL (n.b., the buffer size selection in high-speed routers is justified in [106]).

f) Numerical Results

Figure 5-11 to Figure 5-14 show numerical simulation experiments involving the performance metrics of the router as functions of the high-priority class mean arrival rate in order to assess the performance effect of traffic workload and burstiness of packets classes 1 and 2, as appropriate. More specifically, these experiments evaluate the quality-of-service (QoS) for both classes at the router's Forwarding Function Node 2 with or without the presence of the ACL security mechanism, subject to FCFS and HoL scheduling rules and the CBS and PBS management schemes.

i) Assessing the Effect of the Number of Cores and the Security Component on the Performance of the Router with FCFS-CBS

Figure 5-11 illustrates the comparison of the single-core and quad-core CPUs under FCFS discipline and assesses the effect of the core number on the router performance metrics by focusing on the Class 1 Marginal Mean Response Times, $R_{1,}$ of the router for buffer size N=10. As expected, the quad-core CPU gives the better performance and, clearly, the presence of the ACL security mechanism causes performance degradation at the router. Moreover, the gap between security 'Off' and 'On' vs. performance is reduced in this case by increasing the processing power of the router (i.e., replacing a single-core CPU

with a quad-core CPU achieves a better trade-off between performance and security).

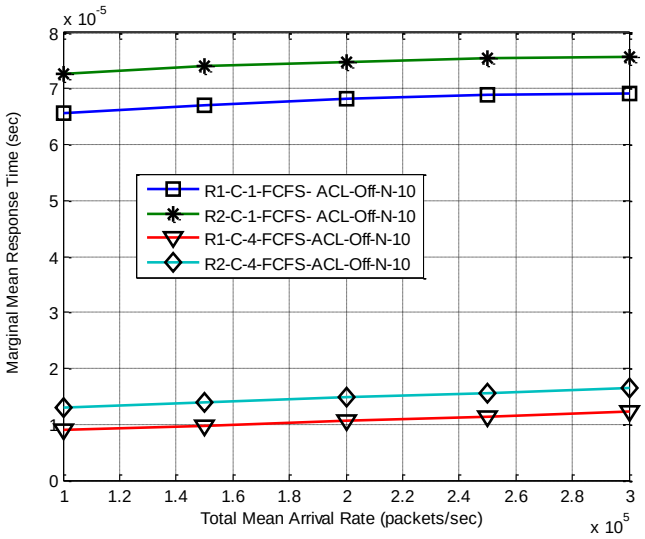


Figure 5-11 Class 1 marginal mean response time under FCFS-CBS for single and quad-core CPUs for router's buffer size N=10

ii) Assessing the Effect of the Number of Cores and the Security Component on the Performance of the Router with HoL-PBS Discipline

An assessment of the effect of the number of cores in CPU with HoL-PBS on the performance of the router for buffer size N = 30 with and without ACL security mechanism is depicted in Figure 5-12 using single- and quad-core CPUs with security 'On' and 'Off'. As expected, the marginal PLP of class 2 is higher than that of the higher-priority class 1 in all cases under consideration. Moreover, this probability decreases for both priority classes once the ACL security mechanism is activated. This is attributed to the reduced input flow of packets at the forwarding engine queue due to the loss of packets that find, on arrival, the ACL security queue at full capacity. It is verified that the gap between security 'Off' and 'On' versus performance is also reduced in this case by using a quad-core CPU. HoL PBS model gives, as expected, better trade-off between performance and security for higher-priority packets.

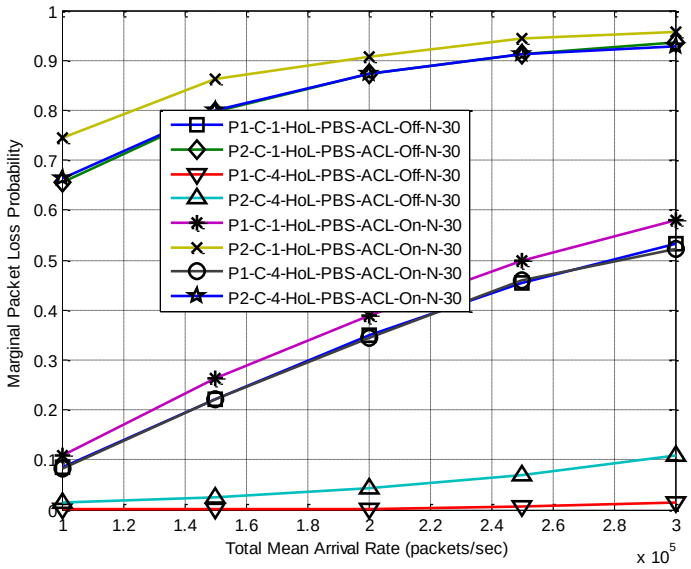


Figure 5-12 Marginal PLP under HoL-PBS for single- and quad-core CPUs for router's buffer size N=30

iii) Comparing the Performance of FCFS-CBS vs. HoL-PBS for Class 1 with and without Security Activation for Buffer Size N=10

Figure 5-13 shows performance comparisons between FCFS-CBS and HoL-PBS for class 1 packets with and without security activation. With a class 2 buffer threshold θ = 30%, the HoL-PBS, as expected, performs extremely well for the high-priority class, especially for quad-core CPUs, as compared with the FCFS-CBS with or without the ACL security mechanism. Moreover, the performance gap between securities 'Off' and 'On' was further reduced in this case by using quad-core CPUs, especially for the high-priority class under the HoL-PBS policy for both single-core and quad-core CPUs.

This indicates that HoL-PBS policy may give, in the presence of a highly bursty traffic of arriving packets (with $C_a^2 > 1$), a balanced trade-off between performance and security for routers in high-speed networks. Cleary, this improvement takes place at the expense of class 2. Thus, depending on the nature of each class application, one may choose to discriminate against the application that is less sensitive to delay and packet loss and also deals with shorter-length packets. Thus, packets of different classes may be broadly served in a way satisfies the required QoS constraints.

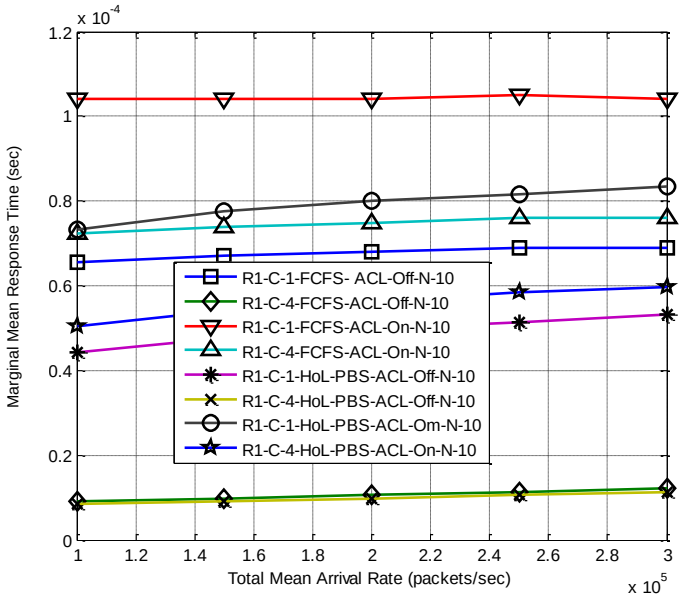


Figure 5-13 Marginal mean response time of FCFS-CBS and HoL-PBS disciplines for both single- and quad-core CPUs for router's buffer size N=10

iv) Comparing the Performance of FCFS-CBS vs. HoL-PBS for Class 2 with and without Security Activation for Buffer Size N=30

Figure 5-14 focuses on the marginal PLP at the forwarding engine queues and shows performance comparisons between FCFS-CBS and HoL-PBS with and without security ACL activation. With threshold fixed to 30%, the HoL-PBS performs, as expected, extremely well compared with FCFS-CBS in the presence of ACL mechanism. Clearly, the marginal PLP is decreased once the ACL security mechanism is activated. This indicates that HoL-PBS gives a good trade-off between performance and security in high-speed network routers, particularly for the higher-priority class. In this way, the most important application may be performed at the required QoS.

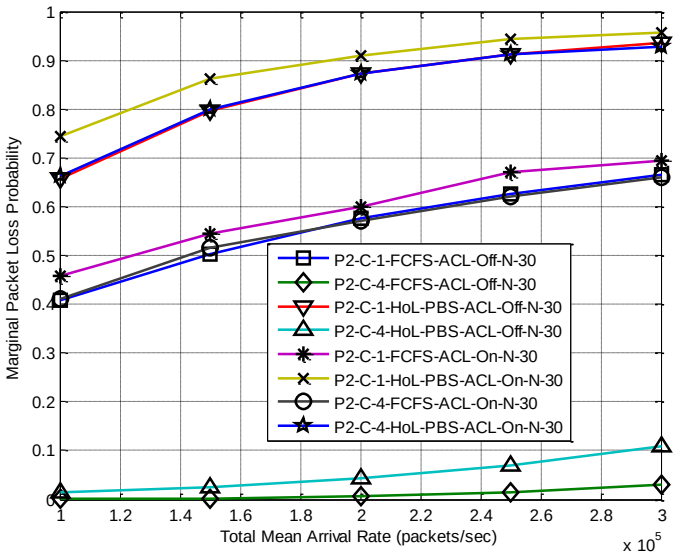


Figure 5-14 Marginal PLP of FCFS-CBS and HoL-PBS disciplines for both single-core and quad-core CPUs for router's buffer size N=30

5.4 ME as a Cost-Effective Methodology for the Trade-off Analysis of High-Speed Routers with ACL

ME [12 , 20 , 90] can be used to analyse a queueing network of M queues, with finite capacity represent high-speed routers with R traffic classes (c.f., [16]), to assess performance vs. security trade-off [74]. This network can be decomposed into M individual queues with R classes, each of which can be analysed in isolation, subject to the evaluation of the blocking-dependent effective service times and overall arrival and departure processes at each router queue. These processes are based on the departing, merging and splitting traffic streams per queue *k* and class *i*, as appropriate. The first two moments of GE for these traffic streams are calculated by the formulae devised in [16 , 20 , 107] and the queues of the routers can be presented, as appropriate, by the GE/GE/c/N/FCFS/CBS, GE/GE/c/N/HoL/CBS and GE/GE/c/N/HoL/PBS building block queues, whose analytic ME solutions can be seen in [16 , 20].

However, the determination of the first two moments of the inter-departure streams for the multiple server queues is analytically complex thus a heavy traffic approximation may be applied in to utilise the corresponding single

server flow formulae (c.f. [16 , 20 , 107]). This concept is depicted for router with ACL in Figure 5-15 for high-speed router with ACL. Thus, multiple servers QN can be approximated by single server queue with total mean service rate, μ_t = $c\mu$ and the same service time SCVs (c.f., [108]).

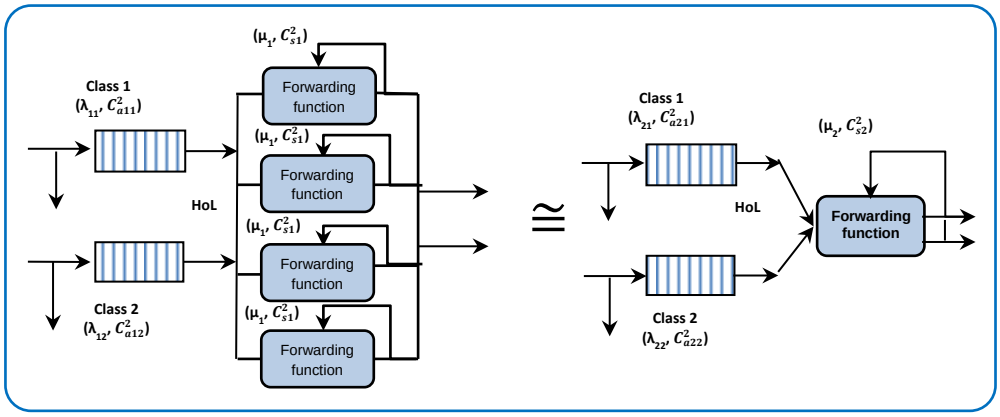


Figure 5-15 Heavy traffic approximation for Forwarding Engine (HoL) queueing system of the high-speed router

5.5 Summary

Performance-engineering concepts were applied, as appropriate, to mitigate the adverse effect of Extended-inbound ACL security mechanism on the performance of routers towards a trade-off between performance and security in high-speed networks under heavy traffic flows condition. In this context, ACL mechanism within the router was modelled in two ways:

Firstly, ***implicitly*** by decreasing the service rate (or the forwarding rate) of the router's CPU by a predefined percentage; and

Secondly, ***explicitly*** by assigning an individual QN node for ACL which is connected in tandem with another QN node representing the forwarding engine queue. RS-FD Blocking mechanism was exploited to reflect the behaviour of ACL security mechanism.

In both models, the queues are GE-type queues with single-core and quad-core CPUs under FCFS and HoL service disciplines for the evaluation of performance-related security via simulation, subject to CBS and PBS buffer management schemes. In the second QN, RS-FD blocking mechanism was

used to explicitly model the ‘Accept-Deny’ behaviour of ACL security mechanism. A comparative numerical study was conducted in terms of two performance metrics: mean response time and PLP.

Although the ACL security mechanism has an adverse effect on the performance of the router, the numerical experiments results indicated that adopting quad-core CPUs enhance the trade-off between performance and ACL security for routers in high-speed networks. Moreover, In particular, the performance gap between ACL security ‘Off’ and ‘On’ was reduced in the presence of highly bursty traffic flows of packets under the HoL-PBS and FCFS-CBS policies incorporating quad-core CPUs, especially for the high-priority class of the HoL discipline, unfortunately at the expense of the low-priority class.

Based on the obtained results, a telecommunications engineer may choose, depending on the nature of each class application, to discriminate against the application that is less sensitive to delay and packet loss. In this way, all classes of packets may be broadly made to satisfy the required QoS constraints. This study is a first step towards establishing a balanced trade-off between security and performance using quantitative means for the design and development of router architectures under bursty traffic conditions. ME principle, was suggested for futurework, as a cost-effective analytic methodology for secure high-speed routers when they are modelled with arbitrary open QNs models in order to investigate the performance and security trade-offs in high-speed routers [20], [16].

The following chapter will present how the quantitative methodology will be extended to appropriately model RANETs in order to investigate their performance and security trade-offs.

Chapter 6 Performance-Related Security Modelling and Evaluation of RANETs Using G-QNs

6.1. Introduction

In a fast-evolving mobile wireless robotic environment, the network infrastructure is most likely to be formed in an ad hoc fashion, especially as robots are most likely to be equipped with low-power wireless transceivers with short range, thus providing additional robustness against the single point of failure of centralized approaches (c.f., [29]). Thus, RANET, with its simplified design, low operational cost and decentralized control, seems to be a most suitable and unique architectural choice for the networked mobile wireless robots and the dynamic nature of their applications (c.f., [29 , 54 , 64]).

Performance and security are two of the main aspects that should be taken into consideration during the design, development, tuning and upgrading of RANETs. Existing metrics and the derivation of new ones are required in order to assess performance-related security and power-saving constraints (c.f.,[54]). Security in RANETs is an important issue due to the associated open medium, implying that “any sensitive sent data between two nodes can be received by other nodes in close proximity” (c.f., [109]). This feature makes RANETs more sensitive to security threats than wired networks. An optimal trade-off between performance and security should lead to the establishment of robust and cost-effective standards for RANETs [54 , 110]. To reduce security threats in RANETs, it is possible to apply some of the existing security protocols used for wired networks, such as the MAC layer WEP protocol (c.f., [64], [111]). Note that WEP is a MAC layer protocol that provides access control in wireless networks and prevents modification and disclosure of data being transmitted (c.f., [10]). WEP introduces extra bits during encryption process and consequently, requires additional delay and consume more power to implement the encryption.

In order to determine suitable trade-offs between performance and security of WEP, and enable efficient and secure communications amongst the robot nodes, this chapter presents a quantitative methodology which is based on the one proposed for high-speed routers, and is extended as appropriate. This extension is made due to the fact that to WEP security mechanisms in RANETs, as infrastructure-less networks are performed at each individual robotic node subject to traffic burstiness as well as nodal mobility. In this context, the proposed quantitative methodology is extended to incorporate an open arbitrary topology QN model of a RANET with Gated queues (G-Queues), where each node models a robotic node with infinite capacity queues and dual CPUs, multiple classes of data packets under FCFS and HoL disciplines and bursty arrival traffic flows characterised by an ICPP(c.f., [20]). SS [11] and PEPs are included in the (G-QN) model in order to establish an 'optimal' performance vs. security trade-off. Moreover, G-Queues are also included within the model to account for node's mobility (c.f., [18], [59]) to enable realistic decisions in mitigating the performance of mobile robotic nodes in the presence of security. The mean marginal end-to-end delay was adopted as the performance metric to indicate the trade-off improvement. Numerical experiments are carried out, based on DES, in order to establish a balanced trade-off between security and performance towards the design and development of efficient RANETs architectures under bursty traffic conditions.

6.2. Performance Evaluation of a RANET with WEP Security and SS

In this section, a case study is presented focusing on DES analysis of a stable open G-QN model of a RANET with WEP security protocol [10] and/or SS (c.f., [11 , 17 , 46]), as appropriate.

The aims of the study are to i) quantify the adverse effect of security on the performance of the ad hoc robotic nodes of a RANET when the WEP security protocol with or without SS functionality is enabled, and ii) establish suitable experimental trade-offs between RANET's performance and WEP security/SS

protocols, based on performance engineering upgrades of the corresponding open G-QN model.

6.2.1 Performance versus Security Trade-off under WEP

The adoption of the WEP protocol involves the employment of extra bits to secure frames and, as a consequence, requires additional processing time, power and memory to perform encryption at a sending RANET node and decryption at a receiving node (c.f., [10]).

To mitigate the adverse effect of security on network performance, SS mechanisms, especially selective encryption, were proposed so that only a percentage, p ($0 \leq p \leq 1$) of data packets will be going through the security process(c.f., [11 , 17 , 46]). In this context, an adaptive performance vs. security trade-off was introduced in [11 , 17 , 46], which also improves power-saving in MANETs. Consequently, a selective WEP security mechanism may also be applied to guarantee the acceptable levels of security in RANETs within required bounds of performance.

In the case study, 'On' and 'Off' WEP as well as selective WEP security with percentage p ($0 \leq p \leq 1$) are taken into consideration for the analysis of the employed open G-QN model towards the establishment of effective performance vs. security trade-offs in RANETs. More specifically, an open G-QN is employed to assess the adverse impact of security on the performance of a RANET, where each robotic node consists of two queueing nodes in tandem - (c.f., Figure 6-1), the first one representing implicit security processing and control under the WEP protocol and the second one for transmission - along with an 'On-Off' gate, reflecting the profile of an arrival process under nodal mobility. Both security and transmission nodes were parameterised through the mean rate and SCV of the service time.

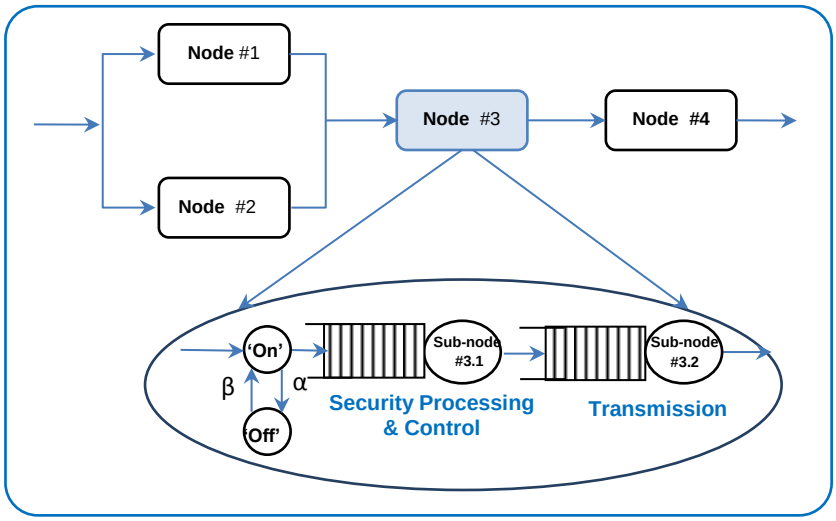


Figure 6-1 A G-QN for a RANET node

6.2.2 The Simulation Analysis for an Open G-QN Model of a RANET

Consider a stable open G-QN model of a RANET with infinite capacity and arbitrary topology comprising N (N ≥ 1) service nodes and R (R ≥ 1) distinct FCFS and HoL classes of data packets, as appropriate. Each node is composed of two sub-nodes, as depicted in Figure 6-2, the WEP queue whilst the second one models the transmission queue.

Channel availability at each WEP sub-node is captured by introducing a gate [18]at the channel entry of the queue of each node. When this channel is broken due to the node mobility, the queue is said to be in 'Off' phase and no arrivals can enter the WEP queue, as the node is no longer connected with the network. When the queue is at the 'On' phase, the arriving packets are allowed to enter the WEP queue for security service. The generic DES algorithm has been implemented in Java and is constructed to analyse the stable open G-QN model of a RANET with infinite capacity and arbitrary topology (c.f., [112]). Each node may have either one or more servers and operates according to either FCFS or HoL scheduling disciplines, as appropriate. Both external inter-arrival and transmission 'Service' times follow the GE-type distributions. In this context, each G-Queue with WEP-based security has an overall ICPP arrival process (i.e., GE-type inter-arrival times and exponential holding times during 'On' and 'Off' periods) modelling the mobility of each RANET node.

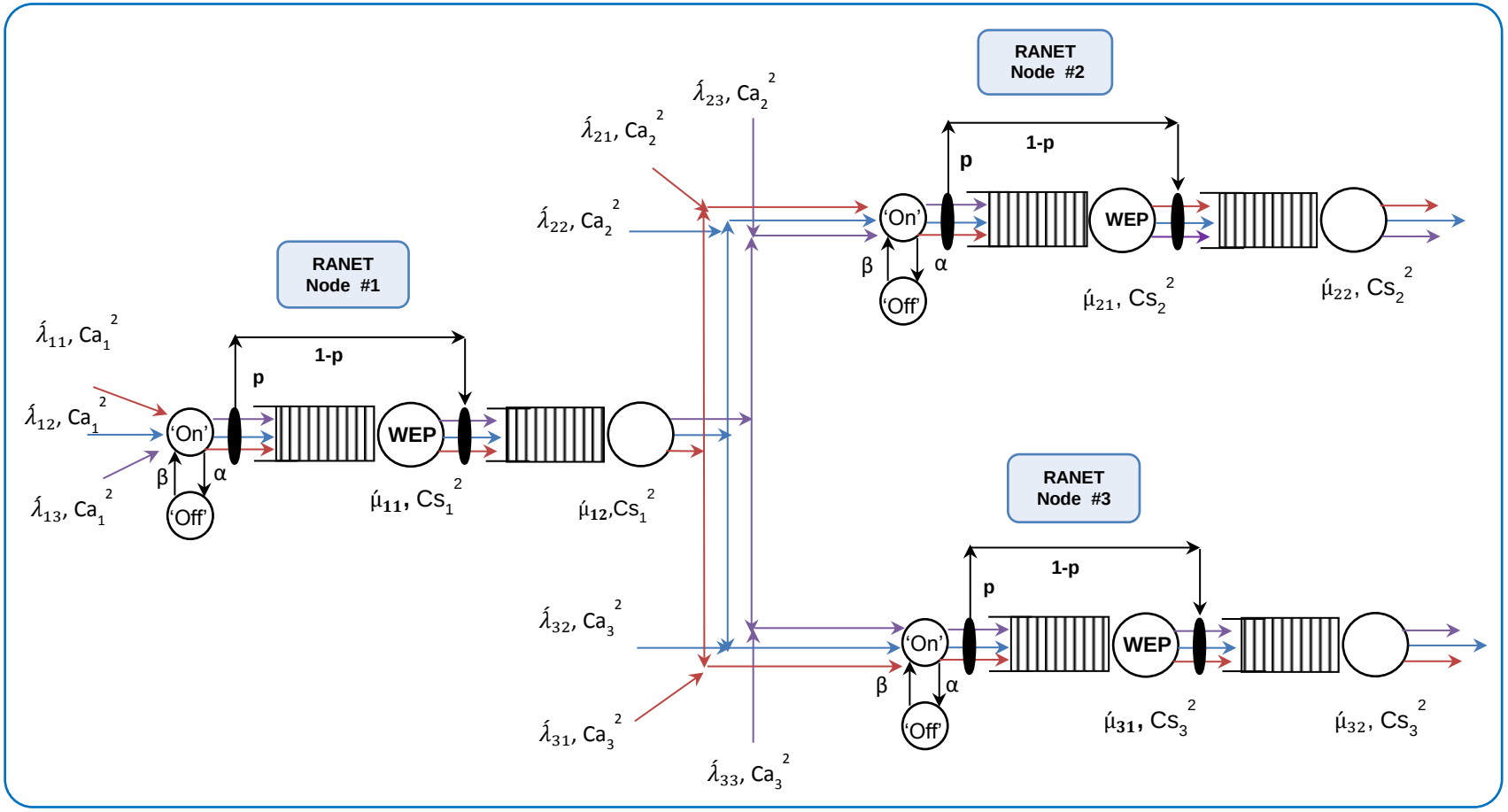


Figure 6-2 A stable open feed-forward G-QN model of a RANET with WEP and SS

Without loss of generality and for illustration purposes, this chapter presents an open G-QN model with feed-forward configuration and three classes of packets (depicted in Figure 6-2 by three different colours: class 1 indicated by red, class 2 indicated by blue and class 3 indicated by purple). Note that the traffic intensity for the network varies from moderate to high values (in the range 0.35 to 0.90). Each transmission sub-node may have a single server or dual servers (as specified in the simulation inputs). The performance metric of the mean marginal end-to-end delay of the stable open G-QN model is adopted and relative comparisons are carried out under various experimental scenarios, where the WEP with SS protocol is activated or deactivated. The simulation scenarios are tabulated in Table 6-1. The three distinct classes with different service requirements considered in this study are displayed in Table 6-2.

Table 6-1 Simulation scenarios

Open G-QN Model of a RANET	Parameterisation
1. Evaluating the adverse effect of security on RANET's performance for single server under FCFS and HoL rules (c.f., Figure 6-3, Figure 6-4)	k→ +∞; $C_a^2 = 40, C_s^2 = 5$; Sec = 'Off', 'On'; c = 1, 2; p = 0, 1; FCFS, HoL.
2. GE-type Performance Bounds for RANETs: Varying the tuning parameter k of the H_2(k) inter-arrival times per class for single and dual server under FCFS and HoL rules(c.f., Figure 6-5).	k = 2, 10, 100, +∞; $C_a^2 = 40, C_s^2 = 5$; Sec = 'On'; c = 2; p = 1 (100% of packets are encrypted) FCFS, HoL.

3. Varying the SCV of the inter-arrival times per class for RANETs with dual servers under FCFS and HoL rules (c.f., Figure 6-6 to Figure 6-8).	k→ +∞;
	Sec = 'Off' / 'On';
	C_a^2= 1, 20, 50, 100, 200;C_s^2= 5;
	c = 2;
	p = 0, 1;
	FCFS, HoL.

4. Improving RANET's performance by utilizing the SS under FCFS and HoL rules (c.f., Figure 6-9 to Figure 6-11).	k→ +∞; Sec ='On'; C_a^2= 1, 20, 50, 100, 200; C_s^2= 5; c = 2; p = 0.5, 1 (50% and 100% of packets are encrypted respectively) FCFS, HoL.

6.2.3 Numerical Experiments

In this section, a series of numerical experiments, based on the simulation scenarios 1–4 listed in Table 6-1and the associated simulation Inputs of Table 6-2is carried out in order to address some of the main performance-related security aspects of a RANET, based on DES analysis of the corresponding stable open G-QN model of Figure 6-2. More specifically, these experiments aim to i) Quantify the adverse performance effect of security; ii) Establish GE-type performance bounds; iii) Predict the adverse performance impact of traffic burstiness, by means of increasing SCV value up to 200, for illustration purposes; and iv) improve RANET performance via WEP when SS with probability p, ($0 \leq p \leq 1$), is 'Off' or 'On' respectively.

Table 6-2 Simulation inputs

Parameters	**Data Values**
Number of Classes	R = 3 classes;
Number of Servers per node	c = 1, 2;
Network topology	Feed-forward (c.f., routing matrix);
Number of RANET Nodes	N = 3 RANET nodes; Sec = 'Off';
Number of RANET Sub-nodes	N = 6 RANET sub-nodes; Sec = 'On';
Number of servers per node	c = 1, 2;
Mean Arrival Rates per class	λ_1 = 100, 400, …, 2200 packets per second (pps); λ_2 = 120, 420, …, 2400 packets per second (pps); λ_3 = 140, 440, …, 2600 packets per second (pps).
SCV of Inter-arrival Times per Class	$C_{a1}^2 = 40$, $C_{a2}^2 = 40$, $C_{a3}^2 = 40$.
Channel Bandwidth (BW)	11 Mbps.
Mean Transmission Time per Packet	Packet size/ BW.
Mean Packet Size per Class (in Bytes) (n.b., Packet Sizes are Exponentially Distributed)	(625,750,875) bytes respectively
Queueing Disciplines	FCFS, HoL.
Mobility Parameters per Node:	
α (transition rate to 'Off' state)	$\alpha_1 = 0.04$, $\alpha_2 = 0.05$, $\alpha_3 = 0.05$.
β transition rate to 'On' state)	$\beta_1 = 20$, $\beta_2 = 10$, $\beta_3 = 10$.

a) Quantifying the Adverse Effect of WEP Security on RANET's Performance

Based on Simulation Scenario 1, Figure 6-3 and Figure 6-4 focus on classes 1 and 2, displaying the marginal mean end-to-end delays of the open G-QN vs. the mean arrival rates of classes 1 and 2 respectively, under FCFS and HoL rules with WEP security 'On' and 'Off' and GE-type inter-arrival and service times (in the simulation, the GE-type distribution is represented as a H_2 (k ~ 10^5) distribution).

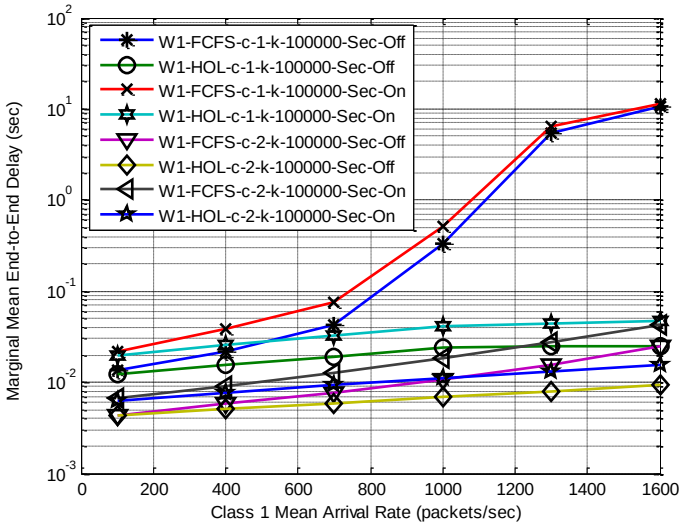


Figure 6-3 Mean end-to-end delay vs. mean arrival rate for class 1 with WEP sec 'On' and 'Off' for an open GE-type G-QN model with single and dual servers under FCFS and HoL rules

Clearly, the WEP security activation has an adverse effect on RANET's performance with the HoL rule, giving the most optimistic value for mean end-to-end delays, for the highest priority class 1. Moreover, under the FCFS rule, the mean end-to-end delays are most pessimistic. The performance of the open G-QN model is improved using dual servers at each forwarding node, where the difference (distance) of the marginal mean end-to-end delays with and without WEP activation is much closer (especially for higher-priority classes under HoL) when a dual server is used rather than a single server. This means that with only using dual server, the secure RANET node will almost produce a marginal delay equal for non- secure node, and this improvement is achieved effectively when HoL discipline is applied, as shown in Table 6-3, as there is not much

difference in the RANETs node delay when WEP is activated, for both single and dual servers. If a quad-core CPU is used, for example, the scale of improvement in performance will be reduced slightly compared with dual server, thus using dual server will meet the QoS required and recue the upgrading cost. It can be said that the positive impact of performance engineering (hardware/software) upgrades of the open G-QN model is of a 'Non-linear' nature (c.f., Table 6-3 and Table 6-4)

Table 6-3 Performance distances: differences between class 1 mean end-to-end delays for single and dual servers with WEP security 'On' and 'Off'

No. of Servers	Performance distance (sec) when FCFS is adopted	Performance distance (sec) when HoL is adopted
c = 1	1	0.0219
c =2	0.01793	0.00616

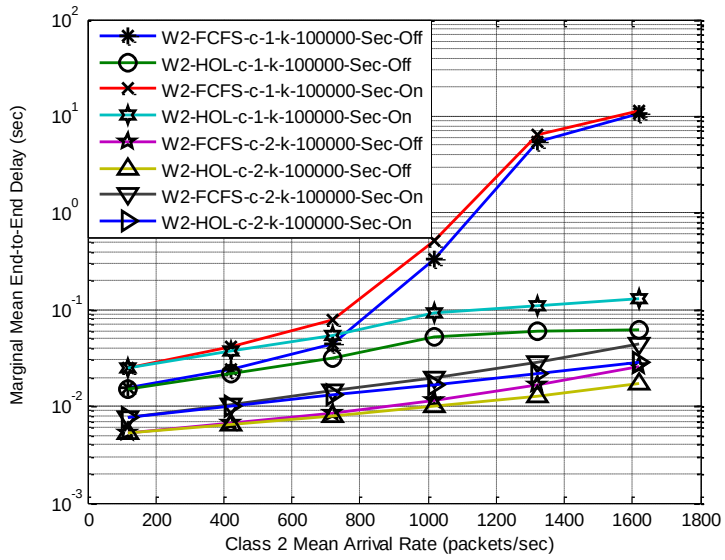


Figure 6-4Mean end-to-end delay vs. mean arrival rate for class 2 with WEP security 'On' and 'Off' for an open GE-type G-QN model with single and dual servers under FCFS and HoL rules

Table 6-4 Performance distances: differences between class 2 mean end-to-end delays for single and dual servers with WEP security 'On' and 'Off'

No. of Servers	Performance distance (sec) when FCFS is adopted	Performance distance (sec) when HoL is adopted
c =1	0.99	0.069
c = 2	0.0175	0.01131

b) Establishing RANET's Experimental GE-type Performance Bounds

Following Simulation Scenario 2, different values of the tuning parameter k of the H_2 (k) family of distributions, namely: k = 2, 10, 100, 10^5 (~ k $\rightarrow +\infty$), are being used in Figure 6-5 to determine GE-type (i.e., k $\rightarrow +\infty$) pessimistic performance bounds for the mean end-to-end delay of class 3 of the open G-QN vs. its marginal mean arrival rate with similar parameterisation as in Table 6-1. It can be observed in Figure 6-5 that the mean end-to-end delay of class 3 increases as the tuning parameter k attains higher values. It becomes apparent, therefore, that, as the tuning parameters k increase, and the effect of traffic burstiness becomes more and more acute. This is particularly true with WEP security activation where extra 'service' time is needed for all data packets to be encrypted. The extremal case of k $\rightarrow +\infty$ gives the worst performance, corresponding to GE-type pessimistic performance bounds (whilst the best-case scenario corresponds to the k = 2), where the delay increases from only 0.03 sec for highly utilised node to around 0.1sec. Note that similar GE-type extremal behaviour has also been observed for classes 1 and 2 (c.f., [20]).

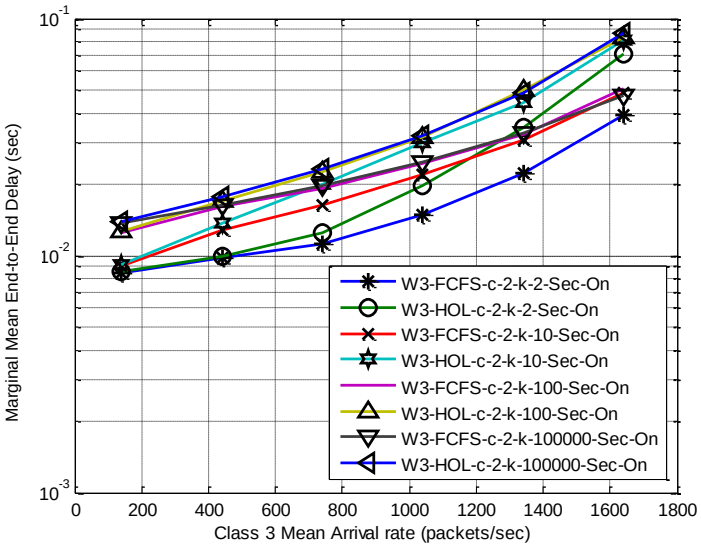


Figure 6-5 GE-type pessimistic performance bounds for the mean end-to-end delay vs. mean arrival rate for an open G-QN model for class 3 over those obtained using H_2(k), k=2, 10, 100, 10^5 distributions with WEP security 'On' and dual servers under FCFS and HoL rules

c) Evaluating the Adverse Effect of Traffic Burstiness on RANET's Performance

Focusing on an open G-QN, which is parameterised according to Simulation Scenario 3 with GE-type external inter-arrival and 'Service' times (c.f., GE ~ H_2 ($k=10^5$)), evaluations of the adverse effect of traffic burstiness on the marginal mean end-to-end delays of classes 1-3 vs. their marginal mean arrival rates, respectively, are shown in Figure 6-6 to Figure 6-8. The results depicted indicate that, as the total mean arrival rate for each class 1-3 increases, the mean end-to-end delay time per data packet with security enabled is relatively much larger than that of the corresponding time without security. Moreover, it is obvious that increasing the SCV of the packet inter-arrival times has an adverse effect of the mean end-to-end delay per class as this leads to the arrival of batches of data packets with increasing geometrically-distributed sizes. The best case is obtained when the inter-arrival times are exponentially distributed with SCV equal to equal 1. The worst performance is attained when the SCV reaches its maximum value of 200.

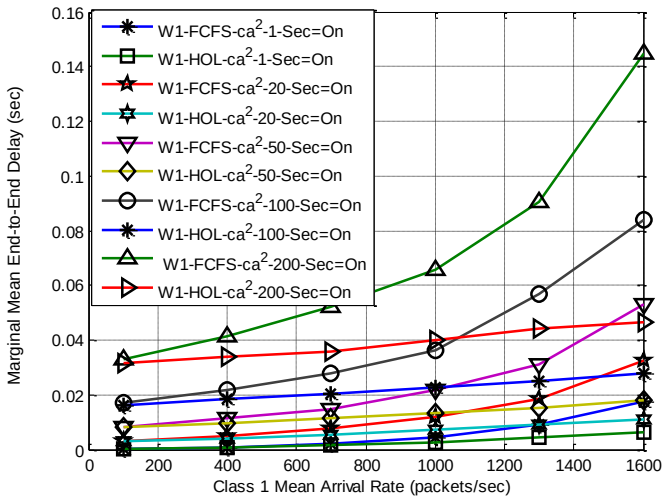


Figure 6-6 Mean end-to-end delay vs. mean arrival rate for class 1 with WEP security 'On' for an open G-QN model with dual servers under FCFS and HoL rules and increasing C_a^2 values

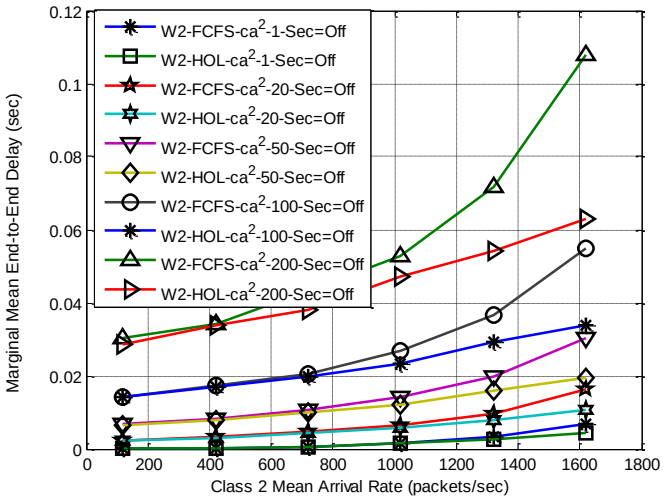


Figure 6-7 Mean end-to-end delay vs. mean arrival rate for class 2 with WEP security 'Off' for an open G-QN model with dual servers under FCFS and HoL rules and increasing Ca^2 values

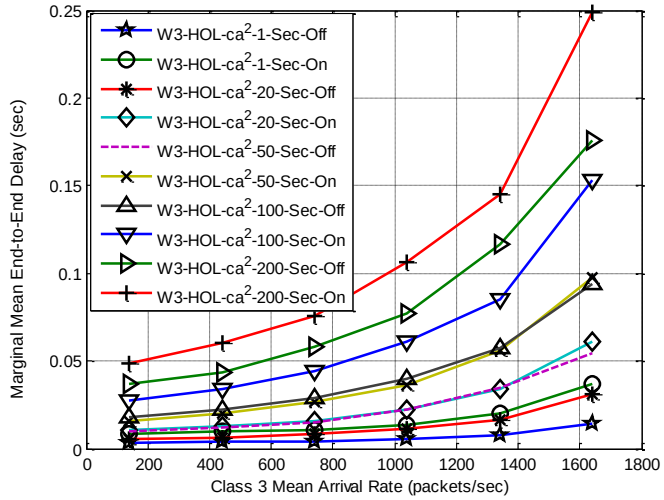


Figure 6-8 Mean end-to-end delay vs. mean arrival rate for class 3 with WEP security 'On' and 'Off' for an open G-QN model with dual servers under HoL rule and increasing Ca^2 values

d) Enhancing RANET's Performance via SS

Adopting the Simulation Scenario 4, Figure 6-9 to Figure 6-11 display the marginal mean end-to-end delays of an open GE-type G-QN vs. the mean arrival rates for classes 1-3, with full and selective WEP securities, respectively. Further to the introduced hardware upgrading from a single to a dual server (in conjunction with the 'Software' upgrade from FCFS rule to HoL rule (in favour of higher-priority classes), the adverse performance effect of security can be reduced further by introducing the selective WEP security (encryption) at each node of the open G-QN. This may be applied to ensure a certain level of security for RANET whilst operating within the required performance bounds. It

is clear from Figure 6-9 to Figure 6-11 that, when p = 0.5 under HoL discipline, the highest priority class has, as expected, the best performance in terms of mean end-to-end delay. This is also applicable for the second priority class whilst, for the third class under FCFS, p = 0.5 gives the best performance. Clearly, HoL under full WEP security provides an improvement only for the highest priority class where the other lower classes have been penalized. In contrast, the SS gives comparable improvements for all classes.

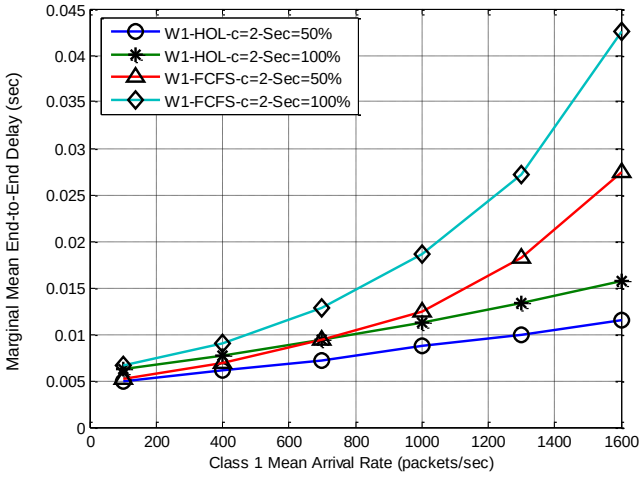


Figure 6-9 Mean end-to-end delay of an open G-QN model vs. mean arrival rate for class 1 with WEP security (100%) / SS (50%) 'On' and dual servers subject to FCFS and HoL rules

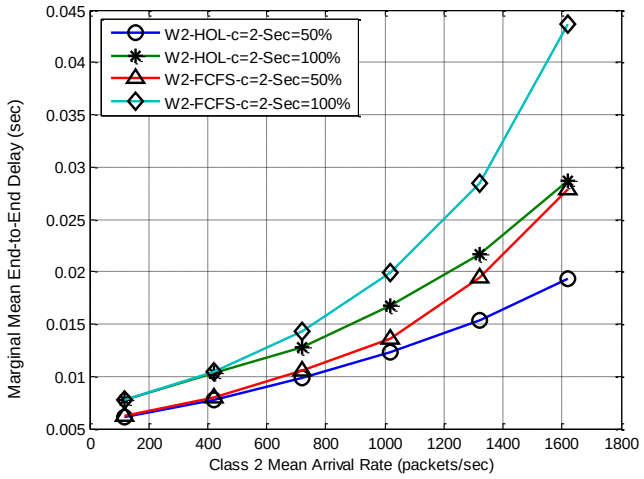


Figure 6-10 Mean end-to end delay of an open G-QN model vs. mean arrival rate for class 2 with WEP security (100%) / SS(50%) 'On' and dual servers subject to FCFS and HoL rules

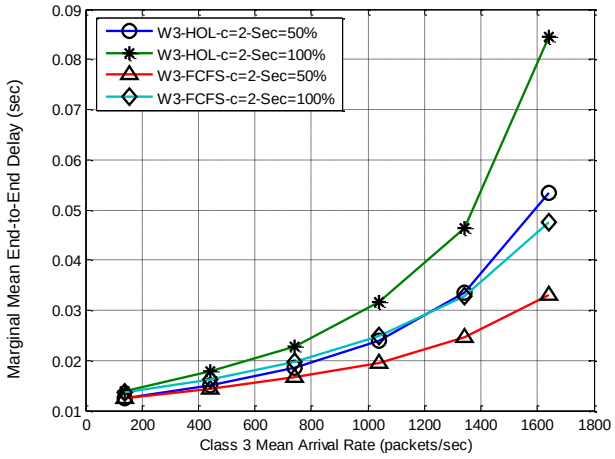


Figure 6-11 Mean end-to-end delay of an open G-QN model vs. mean arrival rate for class 3 with WEP (100%) security / SS(50%) 'On' and dual servers subject to FCFS and HoL rules

6.3 Summary

This chapter presented an investigation into performance vs. WEP security/SS trade-offs in RANETs through the proposed quantitative methodology. More specifically, it was undertaken based on DES analysis of a stable open G-QN model with infinite capacity, arbitrary configuration and multiple classes of data packets, subject to bursty ICPP arrival traffic flows, GE-type transmission times and FCFS or HoL scheduling disciplines. Without loss of generality, typical numerical experiments involving a stable feed-forward open G-QN model evaluated the adverse performance effect of WEP security/SS protocol on the marginal mean end-to-end delay metric per class; moreover, they assessed the enhanced performance impact of a dual CPU and HoL priority rule. It was shown that the distances (differences) between the aforementioned delays when the WEP security is, respectively, 'Off' and 'On' may be significantly reduced, as appropriate, since achieved improvements is of a 'non-linear' nature. This was achieved by the performance engineering of the open G-QN model of a RANET in terms of PEPs (i.e., the acquisition of additional hardware and software resources, such as a dual CPU and HoL rule (c.f., higher priority classes), respectively). In the next chapter, the proposed quantitative methodology for RANETs is further enhanced by introducing a hybrid framework for capturing

‘optimal’ performance vs. security trade-offs for each robotic node by taking more explicitly into consideration security control and battery life by the use of GSPNs.

Chapter 7 Performance and Security Trade-offs in RANETs: Suggestions for Futurework

7.1 Introduction

In this chapter, the hybrid G-GSPN_QN framework is proposed for modelling performance vs. security trade-off in RANETs, at nodal level, to formulate a more advanced quantitative methodology. This framework reflects most of robots hardware components and also security and performance operations at the node. The G-GSPN models security operations and control whilst robotic architectural hardware for intra-robot component to component and inter-robot to robot transmission is represented by a QN. The node's mobility is captured by 'On-Off' GSPN model and the battery charging and discharging is also reflected by a GSPN. Two theoretical case studies on RANETs, adapted from the literature, are presented in order to illustrate the use of QNs to reflect 'intra' and inter-robot communication. In addition, two extended CPSMs are presented as examples to determine the system's parameters that enhance the optimisation of performance vs. security trade-offs in RANETs. Potential usages of the framework for future work are included.

7.2 A Hybrid G-GSPN_QN Model

GSPN model alone is not straight forward for modelling the forwarding part of the RANET node, which includes internal robot operations and control, represented by QN, since a GSPN does not provide simple and direct modelling to accommodate more complex priority scheduling and blocking based strategies (c.f., [95 , 100 , 113]). In addition, the inclusion of a queueing discipline, multiple classes or stochastic routing (c.f., [80 , 99]), blocking mechanisms in a GSPN [85] causes a state space explosion with a complex graph presentation of the network. As a result, the performance analysis of such a model becomes impossible. On the other hand, QNs cannot reflect more

complicated structures such as simultaneous resource possession and synchronisation which are required to model security control [80 , 99].

In order to overcome the inherent limitations of the modelling power of the QN model besides the state space explosion in GSPN, a hybrid modelling framework is proposed for the quantitative analysis of (high-speed network) / RANETs, where each robotic node may be represented by an abstract open hybrid G-GSPN_QN model with HoL priorities, subject to CPSMs. The main advantage of a hybrid GSPN and QN for RANETs is to model more effectively its performance and security behaviour and capture the interaction between the external workload and a RANET limited resource in a simple way.

To this end, the adverse impact of security on the overall performance of a RANET node may be assessed via quantitative analysis, and optimal trade-offs may be established for the evaluation and prediction of the impact of varying model parameters (c.f., [15]) on existing (e.g., [13]) and extended CPSMs.

The general structure of the proposed open hybrid G-GSPN_QN model is depicted in Figure 7-1. This model is composed of an open G-GSPN with a gated multi-class 'On-Off' external arrival process capturing security processing and state-based controls as well as nodal mobility and power consumption. Moreover, it is connected in tandem with an arbitrary QN model with finite capacity channel queues with blocking. The power consumption GSPN sub-model is included to make the framework of RANET more realistic, since the all robot's components (sensors, controllers, actuators and transmission unit) are " power consumers"[114], where sensing, control related computation, motion and communication consume high portions of robot's battery power.

Generally speaking, the exchanged data between robots/nodes can have three different classes for sensory and control messages from other robots besides sensory data from the robot's sensor. Note that the number of classes for sensory data corresponds to the number of external robot's sensor such as

thermal and optical sensors that sense temperature and capture images respectively [22, 23 , 29 , 31].

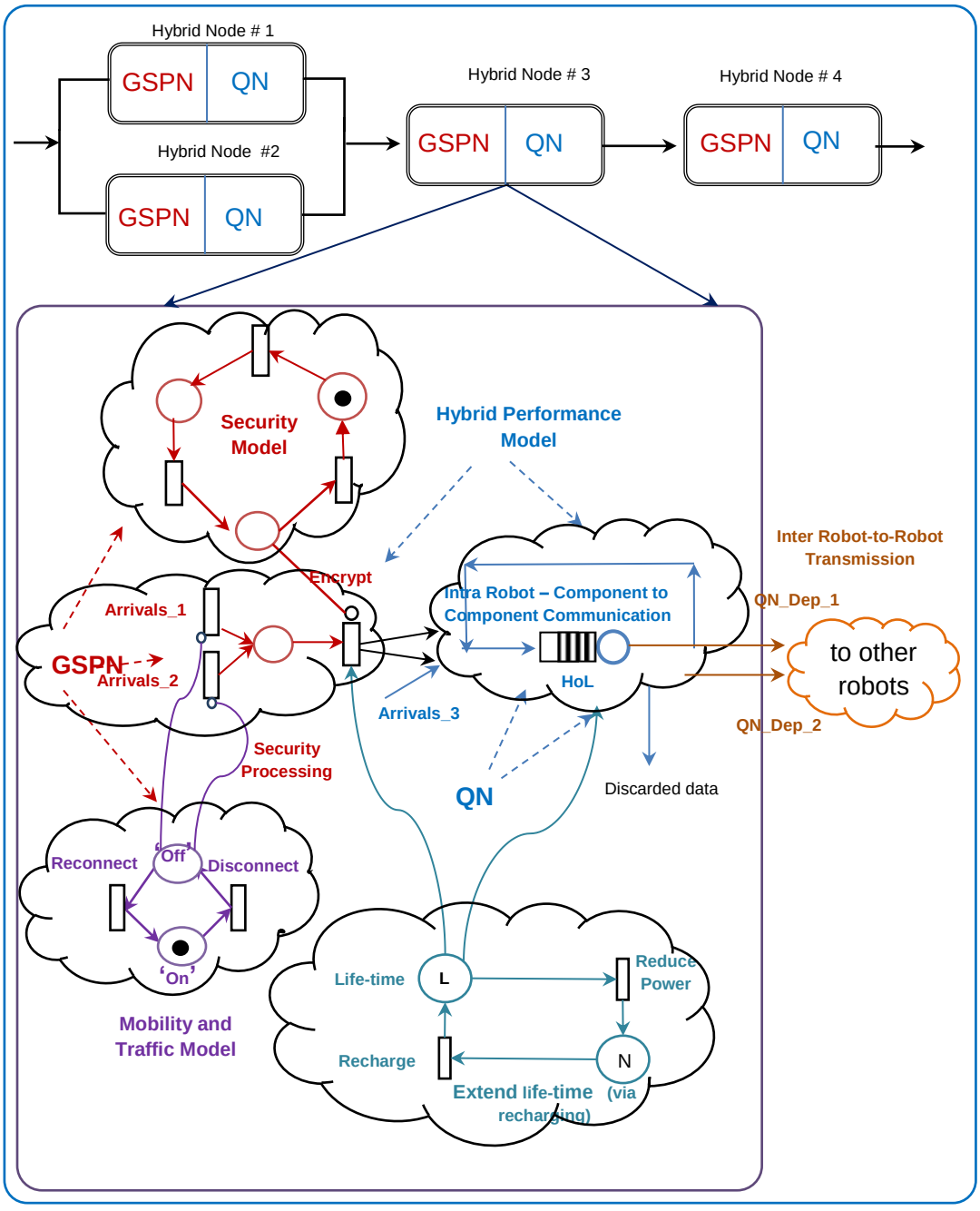


Figure 7-1 An open hybrid G-GSPN_QN model of a RANET node with initial L lifetime of units, finite capacity channel queues and two HoL classes

The three classes are labelled as Arrivals_1 and Arrivals_2 and Arrivals_3 and as shown in Figure 7-1 respectively. The nature of these classes is often 'Application-dependent' i.e., and which application is considered what purpose the study should serve, and QN 'Modelling-level dependent', i.e., how much details to be included in the model to serve that required purpose of study.

The first two classes (i.e., as Arrivals_1 and Arrivals_2), which have two different priorities, go through security check first (security processing GSPN sub-model) then they are passed to QN forwarding sub-model as GSPN_Dep_1 and GSPN_Dept_2 and are processed according to their type. In addition to these two classes, Arrivals_3 class, representing sensory data collected from the environment, arrive and processed by the forwarding QNs sub-model and they are not checked by security processing GSPN sub-model since they are directly acquired by the robot's sensor from its environment (such as video stream or distance measurement made from a particular object). The robot's outputs sent to other robots are represented as QN_Dep_1 and QN_Dep_2.

It is noteworthy that QN_Dep_1 and QN_Dep_2 classes have (often) the same nature of Arrival_1, Arrivals_2 classes received from other robots. In special cases, some of these classes are only considered as input to other robots when we have heterogeneous robots – with different structure and functionality.

Two case studies are adapted from the literature for autonomous robots [22] and a tele-operated robot [21 , 23] respectively, for illustration purposes. They are considered to show the modelling effectiveness of QNs to reflect intra-robot component to component and within a robotic node as well as Inter-robot to robot (or to other nodes) transmission. It is noteworthy that the second case study is a special case of RANETs, since it contains a single robot connected with a tele-operator via relays. However, this can reflect an advantage of the proposed framework possibility of modelling heterogeneous robots/ nodes.

7.2.1 The GSPN-based Traffic and Mobility Model

The traffic and mobility model of a RANET node may be modelled by a multi-class 'On-Off' arrival process of messages represented by IPP (c.f., [69]), when the firing times of the transition is exponentially distributed (n.b., for transitions with GE firing times, the resulting arrival process is ICPP). Thus, as can be observed at the bottom of the diagram in Figure 7-1, there are two places in the proposed GSPN model, which are labelled 'On' and 'Off', relating to nodal

mobility and showing whether or not a robotic node is either connected to or disconnected from other nodes of the RANET. The events leading to these changes are the changes in level of the signal-to-noise-ratio (SNR) of the incoming signal due to robot's movement (c.f., [18 , 59]).

Each arrival process of Arrival_1' and 'Arrivals_2' classes, in security GSPN sub-model, follows an IPP arrival process with an overall inter-arrival time distribution of messages associated with a two-stage hyperexponential (H_2) distribution (c.f., [61 , 62]). As a special case IPP, representing the G-Queue concept, it can be parameterised in terms of GE as the inter-arrival time's distribution. Consequently, GE distribution can fully replace the Gated Queue and represent the node's mobility using the corresponding parameters of IPP (c.f., Appendix B for the corresponding formulae), which leads to the framework's simplification. Moreover, it will be feasible to predict the upper bounds of the performance (which characterises the worst case scenario).

7.2.2 The GSPN-based Security Model

The state transitions of the 'Security' model in RANET node is represented in a general-purpose GSPN model with messages subject to HoL priorities in Figure 7-1. It may be based on group key encryption integrated with IDS (c.f., [15]) towards the protection of the system against both external and internal attacks, respectively. Thus, a security model of this kind is conceived as a generalisation of those proposed in [13]. 'Security' model may be linked with the 'Performance' model by using several inhibitor arcs, as appropriate, to exercise more advanced security control and prevent information leakage (i.e., transmitting messages to be encrypted with compromised keys).

The GSPN can be associated, for example, with 3-states in terms of the encryption key status linked to the security functionality, as depicted in Figure 7-2. To this end, the key is either 'Valid', 'Undetected Broken Key' or 'Detected Broken Key'. Whenever the result of the security check indicates that there is a compromised node, rekeying should take place. If the encryption time

increases, the rate of security incidents is decreased accordingly whilst security detection and system recovery rates are assumed to be fixed. The incident detection normally depends on the quality of the security mechanism adopted such as IDS and its parameters; false positive and false negative probabilities.

As suggested by Wolter and Reinecke [13], the incident rate is adjusted according to the used encryption key. In addition, Cho [15] stated in her model that the detection rate is dynamically adjusted according to the incident rate. Both of these assumptions can be adopted in GSPN security model.

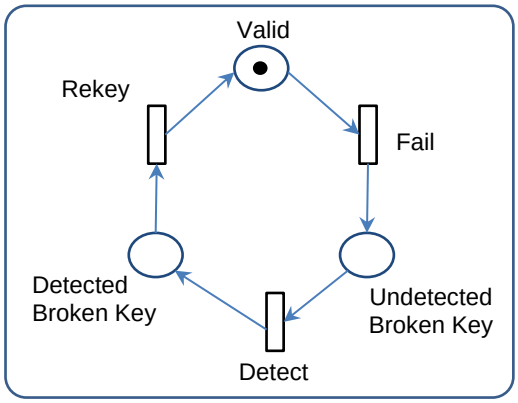


Figure 7-2 3-States GSPN security sub-model

7.2.3 The Hybrid Performance Model

The performance model of a RANET node, shown in Figure 7-3, is of a hybrid nature and is composed of two heterogeneous modelling parts with messages subject to HoL priorities: a GSPN part emulating encryption-based security processing which is called ‘ Security processing GSPN’ sub-model, and a QN part consisting of finite capacity channel queues with blocking for ‘intra’- robot component to component communication and ‘inter’- robot to robot transmission, which is called ‘Forwarding QN’ sub-model’.

a- Encryption-based security processing GSPN Sub-model

The operation of this sub-model is as follows: Once the messages from high or low priority class arrived at the node from the sender, it is then encrypted taking into consideration its priority so that messages with higher priority are served first. If the encryption key is detected as ‘Not Valid’, i.e., broken, the node waits

for a new key to be generated. After the security operations/computations for incoming messages have been performed, the messages are passed to the forwarding QN sub-model for further operations and labelled as GSPN_Dep_1 and GSPN_Dep_2 in Figure 7-3. These classes can be used to control the robot and shared with other robots. Note that the encryption modelling structure using GSPN is very similar to those suggested in [13 , 115]. Encryption delay follows exponential distribution, thus these classes form Poisson process (n.b., this delay can follow any general distribution to reflect traffic burstiness and correlation). It is worth pointing out that the security computations cause the consumption of the limited power battery of the robot, presented in the framework in terms of the battery life time as suggested in [37 , 38]. Thus whenever a message is encrypted, the battery life time is reduced accordingly. This is reflected in the framework by making the 'Life-time' place as input to the 'Encrypt' transition thus the firing of 'Encryption' transition reduce the number of tokens 'L' in 'Life-time' place, as will be explained later in this chapter.

b- Forwarding QN Sub-model

Forwarding QN sub-model can be simple (i.e., single 'server' QN node) or complex (i.e., network of single 'server' queues with arbitrary topology). When a network of queues is used to model the forwarding QN sub-model, it is usually contains the sensor, controller, actuator and transmission units, each of which is represented by a QN node. These queueing nodes are, often, subject to HoL priority classes, with finite capacity thus it can distinguish between the types of the incoming messages and serve the messages with higher priority first. According to the operation conditions and/or application context of modelled robot, FCFS disciple might also be used.

GSPN_Dep_1 and GSPN_Dep_2 messages are passed to the controller (as intra-robot component to component communications), together with external 'sensory' and /or control data Arrivals_3, which to determine whether to share them with other robots via the 'Transmission unit' or to pass them to the

‘Actuator’ to causes the required movement of the robot [30 , 31]. All or selected messages, labelled as QN_Dep_1 and QN_Dep_2, are then transmitted by the robot node, after being formatted as appropriate, for further processing by intermediate nodes or routed for its final destination as ‘Inter-robot to robot communications’.

It is worth mentioning that due to the limited memory of the robot, and especially those involved in monitoring the environment for a long period of time, data are discarded (i.e., overwritten) to save more space for new data [116]. This action is indicated in Figure 7-1and Figure 7-3 by (discarded data).

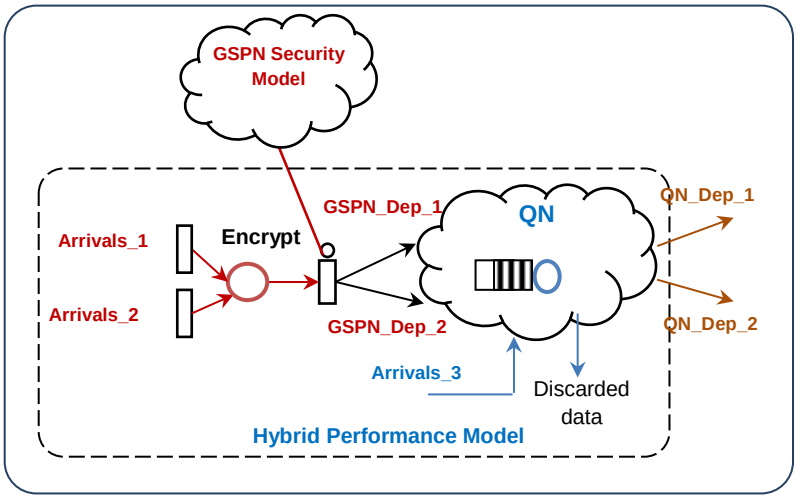


Figure 7-3 The Hybrid Performance Model

Due to the computations / processes made in the forwarding QN sub-model, the robot’s battery life time is reduced. The reduction is a function of the performed process of the robot (e.g., the power consumed caused by the controller and sensing is much less than that caused by motion and transmission) [114]. These various reductions in the power consumption model are reflected the enabling function of the transition ‘Reduce power’ as appropriate.

In the following, two case studies are adapted, for illustration purposes, from [21 , 23] and [22] for autonomous robots and a tele-operated robot respectively in order to explain the modelling and operation concepts of RANET in the context of the proposed framework. In particular, these case studies are considered to show how intra-robot component to component and inter-robot to robot

communication can be reflected by an ‘Application-dependent’ and ‘Modelling-level-dependent’ QN model.

In the first case study, adapted from [22], number of robots communicate according to ad hoc network and work co-operatively to collect and exchange control and sensory data messages between them in order to build 3-D maps of unknown place. These data are assumed to be secure with WEP protocol.

In the second case study, adapted from[21 , 23], a single robot is remotely controlled by a tele-operator to perform navigation/ monitoring task by means of capturing video data of a place and send it back to the tele-operator who has full control of the robot. In order to extend the coverage area for the robot, intermediate mobile nodes are used (acting as relays).

It is worth pointing out that the second case study is a special case of RANET, where a single robot is involved in performing a particular task. However, in the context of this thesis, this case study explicitly shows the flexibility of the proposed framework in modelling heterogeneous structures and functionalities of robots /nodes. In both case studies, power consumption of the robot’s battery is not taken into consideration.

i- Case Study 1

This case study on autonomous robots adapted from [22] to show how to model intra and inter robot communications using QN model. This type of robots has full control of co-operate data sensing and exchanging to perform a common task as well as controlling robots’ motions to a particular target.

1. Application Context

A group of robots co-operatively navigate an unknown place and build its 3-D map. Each robot is provided with a range sensor. The 3-D map is updated according to measurements from its own range sensor (which are the dimensions measured from the robot’s position to a particular obstacle) and localisation module (i.e., the information of the robot’s position -within the map-

at which these measurements are made) besides the received measurement made by other robots. Only necessary measurement information, selected- for example- with probability p as defined by the adopted cooperation probabilistic strategy, are shared with other robots. This information is assumed to be secured with WEP protocol to provide information confidentiality. The updating process of the 3-D map besides sharing information can be affected by security computations as well as the transmission media. Thus, accurate modelling of intra and inter-robot communications will help in evaluating performance and security trade-offs.

2. The robot's Components

In the following, the different components of a single robot and the operation/ interaction of robot's nodes are described. The robot's is assumed to have a 'Sensor', 'Controller', a 'Localisation unit', and an Actuator 'and 'Transmutation unit'. The 'Sensor' provides the sensory and control data to the robot. The 'Localisation unit' gives the robot's position with respect to its surrounding area. The 'Controller' processes incoming data and produces the required response to the actuator which accordingly changes the robot's position to a new selected 'Exploration viewpoint'. In the same time, selected data are transmitted to (shared with) other robots via 'Transmission unit'.

3. The proposed QN

This section describes the proposed QN model for the scenario described above. In particular, it provides information on the input traffic flow to the QN sub-model as well as the components of the proposed QN model and how they interact.

a. The input Traffic Flow

Each robot receives four classes for data and position measurement as input and they are assumed to have exponential inter-arrival time process. The first two classes for data and position (control) measurement made by other robots indicated by brown lines and labelled as GSPN_Dep_1, GSPN_Dep_2 in Figure 7-4. These data come from GSPN sub-model after being checked for

WEP security. In addition, each robot acquires the other two classes measurement and control (i.e., position data) from its sensor and localisation modules respectively, indicated by blue lines and labelled as Arrivals_3 and Arrivals_4 in Figure 7-4. The received data presented by the four classes (GSPN_Dep_1, GSPN_Dep_2, Arrivals_3, Arrivals_4) have different priorities, thus HoL discipline is assumed for both '3-D map update' and 'Transmission unit'. The sensor and actuator, on the other hand, are assumed to act according to FCFS discipline since they served event according to their occurrence time.

b. The Components of the Proposed QN

The corresponding proposed QN model of the forwarding sub-model of the robot is composed of four single-server QN nodes, namely:

'3-D map update' which receives the four classes data (GSPN_Dep_1, GSPN_Dep_2) for received sensory and control data, and (Arrivals_3, Arrivals_4) for the acquired data by the robot' sensor and updates the 3-D map of the navigated place accordingly to determine the new position of the robot;

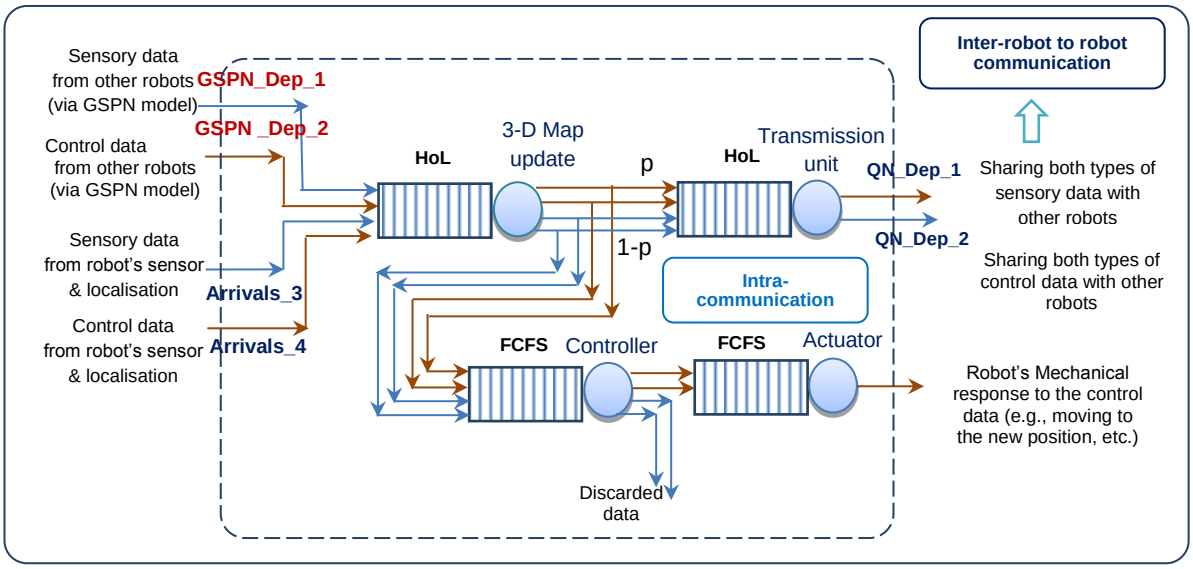


Figure 7-4 QN model for the intra-communication and inter- robot to robot communications

'Controller' which receives data from the robot's sensor (Arrivals_3, Arrivals_4) as well as the output of '3-D map update' queue;

‘Transmission unit’ sends the selected measurements to be shared with other robots (indicated by QN_Dep_1 and QN_Dept_2), and

‘Actuator’ which is a mechanical part such as electric motor that causes robot’s movement.

It is worth mentioning that data acquired by the robot itself are assumed to have higher priority over the received data from other robots. In order to simplify the model, the ‘Sensor’ and ‘Localisation unit’ are considered as sources of data thus they are not presented as queueing nodes in the model.

c. The QN Component’s Operation/ Interaction

The incoming data from security GSPN sub-model and from the environment to ‘3-D map update’ queue and are utilised to update the map then they go through the ‘Controller’ which process data according to FCFS discipline since they are served according to their occurrence time. Selected data, according to the adopted cooperation strategy, are shared with other robotic nodes with probability p while the remaining data are discarded with probability (1-p), after passing through the ‘Controller’. The position information (which is control data) is passed from the ‘Controller’ to the ‘Actuator ‘unit while measurements data are discarded. Only selected sensing measurements are shared with other robots through the ‘Transmission unit’ and they are transmitted according to HoL discipline to preserve class-priority. Based on provided data to the ‘Actuator’, the robot is moved towards the new position. Upon reaching that target, the robot repeats the whole process with a new measurements provided by the sensor from its new position. 3-D map creation and update involve two steps and require keeping some measurement data within this unit. From the modelling-level point of view, for model simplicity, these two processes are combined in a single QN node ‘3-D map and Update’.

d. The QN output traffic flow

The output classes (QN_Dep_1, QN_Dep_2) from QN sub-model should be similar to those represent its input traffic classes to the robot (Arrivals_1,

Arrivals_2). This is considered in the design where QN_Dep_1represents sensory data (aggregated from the robot itself and other robots) and QN_Dep_2 represents control data (aggregated from the robot itself and other robots).

ii- Case Study 2

This case study, adapted from [21 , 23], is for a tele-operated robot which is assumed to be communicated with tele-operator according to ad hoc network technology to perform navigation tasks. In this context, the robot is assumed to be totally controlled by the tele-operator who might be able to communicate directly with the robot or it might be far from it. In the latter case, intermediate nodes, which are assumed to be mobile, are used to deliver data between the robot and tele-operator. Despite having only one robot in this case study, an assumption of having multiple robots with multiple operators can be made as proposed in [117]). This case study can be generalised to account for robots communications. This might be made through semi- autonomous robots with multiple tele-operators.

1. Application Context

The operation of the robot is as follow: the robot captures video from the surround area using video camera and sends it back to the tele-operator. As a response, the tele-operator can display this streaming video and sends back control data to the robot in order to move to the required position. In this case, there are two communication cases:

Video captured by the robot's camera together with tele-operator control traffic, which all are secured by using WEP protocol during transition, are forwarded between robot and other relays nodes in ad hoc manner. Tele-operator can either communicate directly with the robot if they are in the same coverage area or via other mobile nodes that extend the coverage area.

Traffic transmission is delayed due to the transmission media and WEP security computations. As a result, 'Timely control' of the robot might not be feasible. Thus it is of importance to investigate a balanced trade-off in which

transmission delay is reduced while preserving reasonable security level and video quality.

2. The Robot's Components

The robot itself is composed of four parts: '**Sensor**' which is the video camera, '**Controller**', 'Actuator', to allow the robot to move and the '**Transmission unit**' which transmits back video data to the operator (either directly or via other nodes). It is assumed that video data goes from the robot towards the tele-operator while control data goes from the tele-operator towards the robot.

3. The Components of the Proposed QN

This section describes the input traffic flow to the QN sub-model as well as the components of the proposed QN model and how they are interacting.

a. The Input Traffic Flow

There are three types of traffic that present the input to the robotic node, as shown in Figure 7-5. All of these classes are assume to have exponential inter-arrival time process. The first two classes are 'Control data received directly from tele-operator', indicated by GSPN_Dep_1 in Figure 7-5, in order to control the movement of the robot and 'Forwarded control data from other nodes', indicated by GSPN_Dep_2 in Figure 7-5. These classes are passed from the GSPN sub model to QN after being checked by WEP and they have the same priorities. The third class is the 'Video data from robot's camera', indicated by Arrivals_3 in Figure 7-5, and since this data is acquired directly by the robot, there is no need to check it by WEP security protocol. This class is assumed to have lower priority while both control data classes have higher priority.

b. The QN Components

The corresponding proposed QN model for the robot' forwarding part for this case study is depicted in Figure 7-5. The proposed QN model is composed of a **'Sensor'** which is the video camera, '**Controller'**, '**Transmission unit'**, and **'Actuator'.**

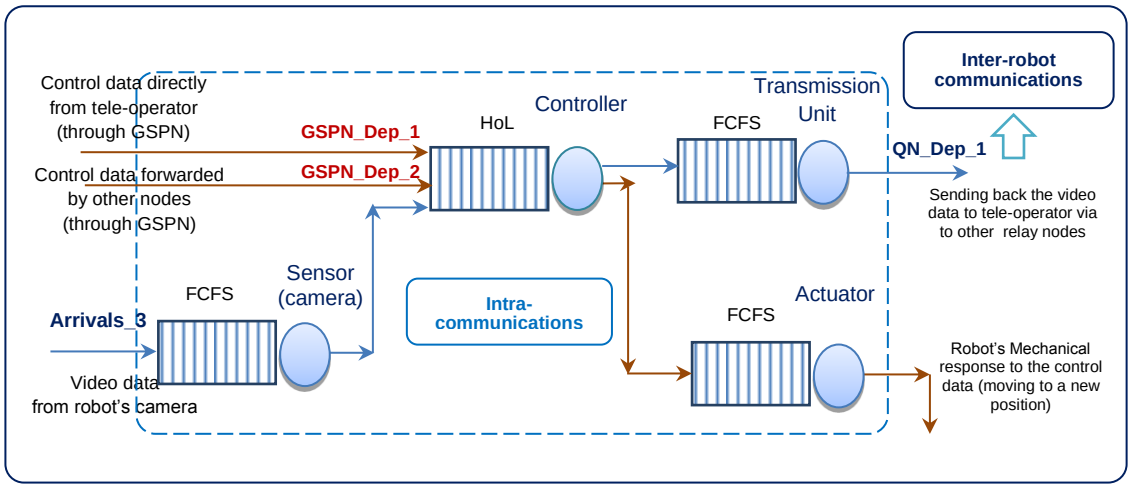


Figure 7-5 QN model for intra and inter robot communications

c. The QN Component's Operation/ Interaction

Both control classes Arrivals_1 and Arrivals_2 are received from GSPN security model and they enter the 'Controller' queueing node as GSPN_Dep_1 and GSPN_Dep_2. Arrivals_3, on the other hand, is received by 'Sensor' queueing node and it is then passed to 'Controller' node. Since these classes have different priority, HoL is assumed to be the queueing discipline for the 'Controller' node. These data are then processed and interpreted by the 'Controller' which convert them to motion commands and passes them to the 'Actuator', which in turn, moves the robot as required.

d. The QN Output Traffic Flow

The output class (QN_Dep_1) from QN sub-model represents video data sent back to the tele-operator by the robot node. Unlike the previous case study, video traffic is assumed to go in one direction (from the robot to the tele-operator), since other intermediate nodes are not robots; they act as relays to only forward video and control data. Note that, in the case of modelling these relay nodes, both 'Sensor' and 'Actuator' queueing nodes should be excluded. The input classes to the 'Controller' within relay QN model are 'GSPN_Dep_1' and 'QN_Dep_1'. The features of 'Controller' and 'Transmission' queueing nodes are the same as those of the robot QN model. The output control and

video data classes are sent by the ‘Transmission unit’ to the robot and tele-operator respectively.

iii. Further Remarks

When a large network of robots with multiple classes, queueing disciplines and routing and blocking mechanisms is modelled and theoretically analysed by pure GSPN, the corresponding state space will explode [80 , 85 , 96 , 97 , 118 , 119]. The resulting pure GSPN model becomes “graphically complex” and not comprehensible [96]. This is due to the increase of number of places/transitions required to reflect these aspects. Moreover, the GSPN cover more details (such as concurrency and synchronisation) than QN and this requires more state space. Therefore, the use of QN model to reflect, in a simple way, the forwarding model of the robot that involves the forth mentioning modelling aspects will eliminate this problem.

When simulation is used as evaluation tool of the hybrid GSPN and QN model compared with pure GSPN, QN effectively reduce the time required to complete the simulation [102] due to its simpler topology and smaller associated event list and it can decrease implementation complexity of the overall simulation code.

7.2.4 The Power Consumption Model

As depicted in the proposed G-GSPN-QN model of Figure 7-6, the power consumption model of a RANET node may be modelled by the battery’s lifetime representing the number of tokens in the power place assigned to each node according to uniform distribution (c.f., [120]).

In this context, the number of tokens in the place ‘Life-time’, L (L > 0), represents the robot’s battery lifetime and it is an input place for the transition ‘Power Reduction’ consuming power with, say, an exponential delay. Security protocols requiring computations together with the transmission process of messages will contribute to more power consumption of the battery and, thus, reduce progressively the number of remaining tokens (units of time) in the input

place ‘Life-time’ for the transition ‘Power Reduction’ it could include a check of departure events of the internal components queueing nodes within the forwarding QN each of which has its own reduction rate. For example, the power reduction rates of the robot considered in [114] are: Motion 12.1%-44.6% Sensing 1.9%-5.1% Microcontroller 14.8%-28.8%. In terms of simulation, these reduction percentages can be included in the enabling function expression of ‘Reduce power’ transition. In addition to previously mentioned sources of power consumption, a fixed reduction rate of the battery life time is applicable when the robot is idle (c.f., [114]).

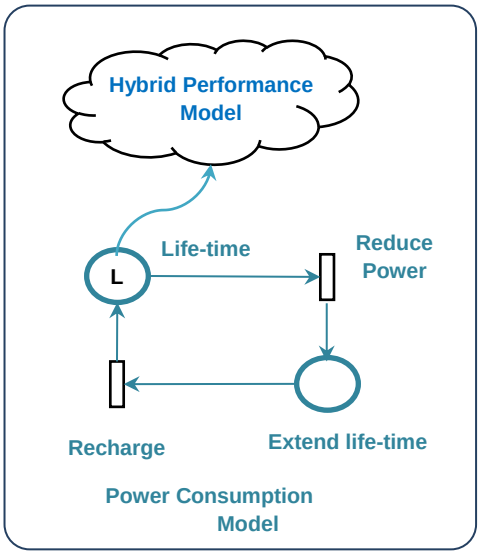


Figure 7-6 Power consumption GSPN sub-model

It is noteworthy that robot’s battery might be recharged [114] when its remaining lifetime reaches a predefined threshold. This event is represented in the GSPN model by the ‘Recharging’ transition and it is defined in the transition enabling function. This mechanism enables the robot to resume its task effectively without being interrupted or stopped due to battery exhaustion. In addition, multimedia traffic can be handled effectively without concerns about power consumption.

The use of the power consumption model gives an indication of the adverse impact of security and transmission computations on the ‘Life-time’ reduction of the robot’s battery. In particular, determining the optimal length of encryption

keys vs. power consumption trade-offs may enable the battery to maintain energy levels for longer and, thus, benefit the operational efficiency of real-life applications.

7.2.5 Extended CPSMs

In the context of the encryption protocol modelled using the proposed hybrid framework (c.f., Figure 7-7) and for illustration purposes, two extended CPSMs are introduced, namely CPSM-Maximum and CPSM-Minimum, based on CPSM proposed by Wolter and Reinecke [13]. These CPSMs may be utilised to determine in order to determine the optimal encryption time.

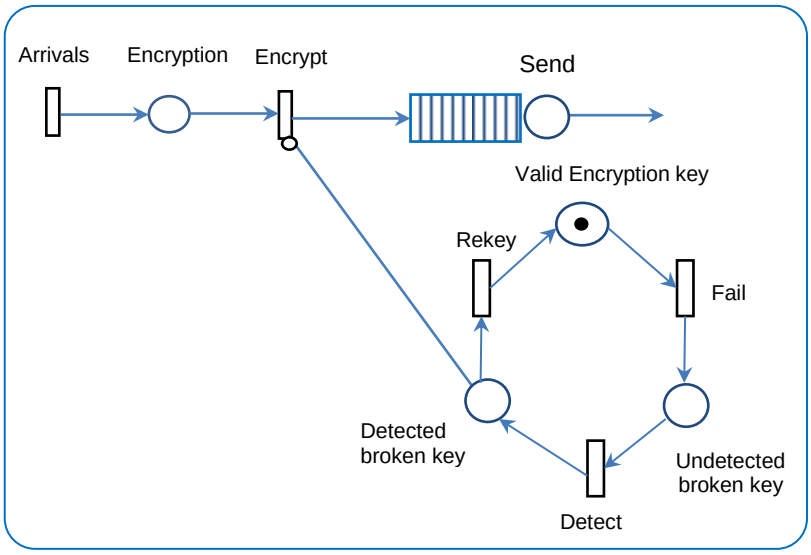


Figure 7-7 Hybrid QN and GSPN model

The general idea behind extending the metric proposed in [13] is to select performance metrics, which are compatible in scale of magnitude, such as utilisation and PLP. Thus, this will prevent the performance metric dominating the overall value of the CPSM when added the security metric represented by probabilities (such as probability of the key to be valid).

Focusing on the CPSM-Maximum, the performance and security metrics, such as system utilisation and probability of having a valid encryption key, respectively, are combined together by adding them. Alternatively, for CPSM-Minimum, the combined performance and security metrics, such as the PLP

and probability of key breaking, are also added together but their combined metric has to be minimised.

In this context, for illustration purposes the following CPSMs are defined:

- $CPSM_1$ is defined as 'the sum of the utilisation of the QN model plus the probability of the system being in a 'Valid' place (or 'State'). This metric may be used to determine a maximum utilisation (which gives an indication of maximum encrypted messages ready to be transmitted) when the system is secure, i.e., having a valid key. This metric can be seen as a CPSM-Maximum expressed by

$$CPSM_1 = Utilisation + P(Valid\ Encryption\ Key)$$

- $CPSM_2$ is defined as 'the sum of the PLP in the encrypting place plus the probability of the system being in 'Undetected Broken Key' place. $CPSM_2$can be seen as CPSM-Minimum and it should give a *lowest possible* PLP in 'Encryption' place when the system is under undetected attack, i.e., the encryption key is broken. Clearly, this combined metric is expressed by

$$CPSM_2 = PLP\ in\ 'encryption'\ place + P(Undetected\ Broken\ Key)$$

In the following sections, numerical experiments are carried out to show the behaviour of the extended CPSMs and how they are affected by the traffic burstiness.

The arrived messages to the model are assumed to have single class. In addition, the firing time of 'Arrivals' transition has GE distribution with SCV=1, 50 and 100, while the firing times of other transitions and the 'send' service times are exponentially distributed. Input parameters for the model used to determine the suggested CPSMs are listed in Table 7-1.

In the following, the CPSMs are firstly plotted together with their corresponding individual performance and security metrics. Then, the impact of messages inter-arrival times burstiness on these metrics is assessed.

Table 7-1 Input parameters of hybrid QN and GSPSN to determine $CPSM_1$ and $CPSM_2$

Parameter	Value
Arrivals	8 messages per sec
Encrypt	0.01 to 0.34 step 0.01 sec
Fail (time to key breaking)	1.25, 25, 50, 100, 600 to 15100 step 500 sec
Undetected Broken key	12 sec
Rekey	36 sec
Send	10 messages per sec
SCV of inter-arrival times	1, 50, 100
Capacity of 'Encryption' place and 'Send' queue buffer	100

a) The behaviour of the extended CPSMs

Figure 7-8 depicts $CPSM_1$ and its components, i.e., the utilisation of the QN model (indicated by the blue curve) and the probability of the encryption key being valid (indicated by the green curve).

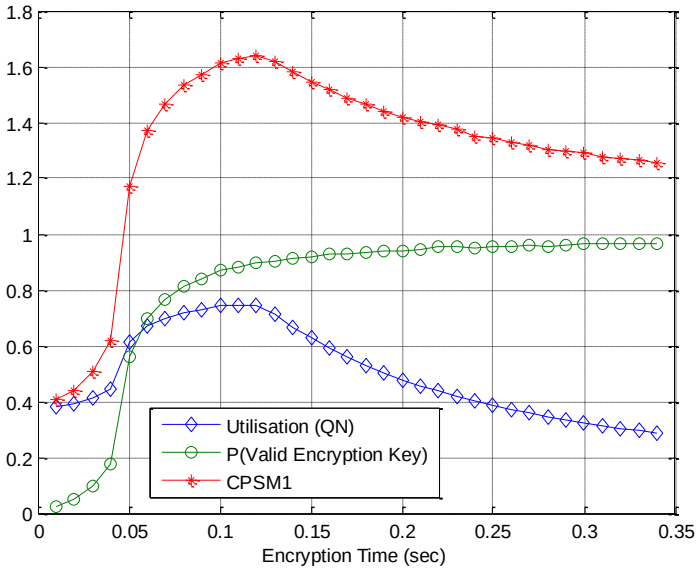


Figure 7-8 $CPSM_1$ when SCV of messages inter-arrival times is equal to 1 [1]

For low encryption times, messages do not wait for long times to be encrypted. Since the security level is low, the key can be broken easily. As the encryption times increase, messages begin accumulating waiting to be encrypted. Consequently, this leads to an increase of the overall delay and thus, a

considerable decrease in the throughput and utilisation of queue ‘Send’. However, beyond a particular encryption time (or consequently for an encryption key length), the security level will be almost the same (c.f., [13]) but increasing the key length will definitely decrease the utilisation as described earlier. It is clear that the probability of the key being valid increases linearly with encryption time as it is related with the time to next security failure, i.e., key breaking. For the considered model, optimal encryption time according to $CPSM_1$, which gives an optimised performance and security simultaneously, is around 0.13 sec.

Figure 7-9 shows $CPSM_2$ and the corresponding metric which are PLP in ‘encryption’ place and the probability of the system being in ‘Unetected broken key’ state. The increase in the encryption times causes the accumulation of messages in place ‘Encryption’ and due to its limited capacity, messages are lost. Thus it is vital to minimise the probability of the key being compromised which leads to system recovery. There is an optimal encryption time at which the encryption process is fast enough and the corresponding key is secure enough so that it cannot be broken easily. At this time, PLP is at its minimum as well as the key breaking rates. Beyond this time, messages accumulate in a linear manner, and so the PLP, in ‘Encryption’ place which is further increased whenever the system is recovering from a security failure which causes encryption suspension. When the place ‘Encryption’ becomes full, new arrived messages are lost and therefore the overall number of messages, as well as PLP, remain unchanged. In contrast to short keys, longer encryption keys are more secure thus they are less likely to be broken. Therefore, the probability of ‘Undetected Broken Key’ is decreasing as a function of encryption times.

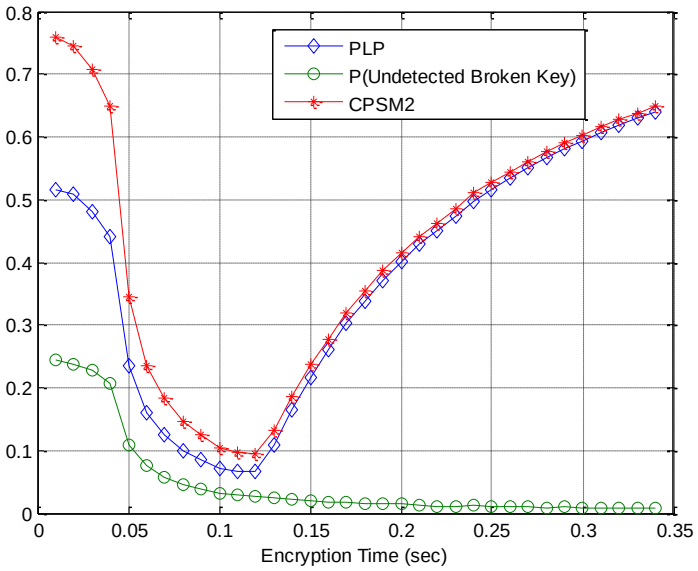


Figure 7-9 $CPSM_2$ when SCV of messages inter-arrival times is equal to 1 [1]

b) Impact of SCV on Extended CPSMs

It is worth mentioning that the probabilities of the key being valid, undetected as broken or detected as broken by the system are not affected by the change of the traffic burstiness. Thus the change in performance components of the extended CPSMs causes the change of the combined metrics.

Figure 7-10 depicts $CPSM_1$ for different degrees of traffic burstiness. It is clear from the figure that $CPSM_1$ has an obvious maximum when the traffic burstiness is low, i.e., when SCV = 1 where the inter-arrival times are exponentially distributed. However, when the burstiness degree increases, the utilisation will decrease due to the increasing messages loss and therefore $CPMS_1$ curves are shifted down accordingly. It is noteworthy that $CPSM_1$ curve becomes flatter which hides its maximum value and this behaviour is caused by the system being overwhelmed.

Since the probability of having a 'valid' key is independent of the SCV impact, the overall combined metric will remain the same.

The increase of the traffic variability shifts the optimal encryption time to higher values according to the corresponding SCV. Therefore, it can be concluded that longer encryption keys are needed for traffic with higher burstiness degree.

It is also clear that the curve is shifted down with increased traffic burstiness since the system throughput decrease accordingly.

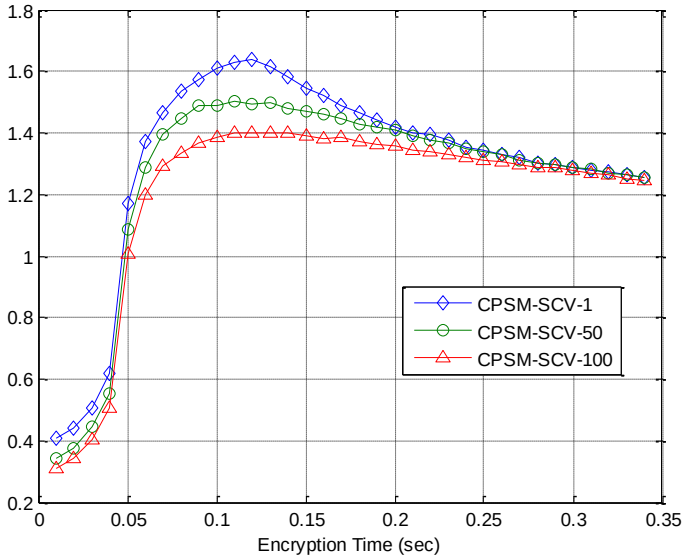


Figure 7-10 $CPSM_1$ for difference SCV vlues ofmessages interarrival times [1]

Figure 7-11 shows the impact of increasing the degree of traffic burstiness on $CPSM_2$. It is obvious that higher the burstiness of traffic the more messages are entering the system and this leads to higher PLP and therefore the curves are shifted up. Similar to $CPSM_1$, the increasing of the traffic burstiness requires longer encryption key lengths.

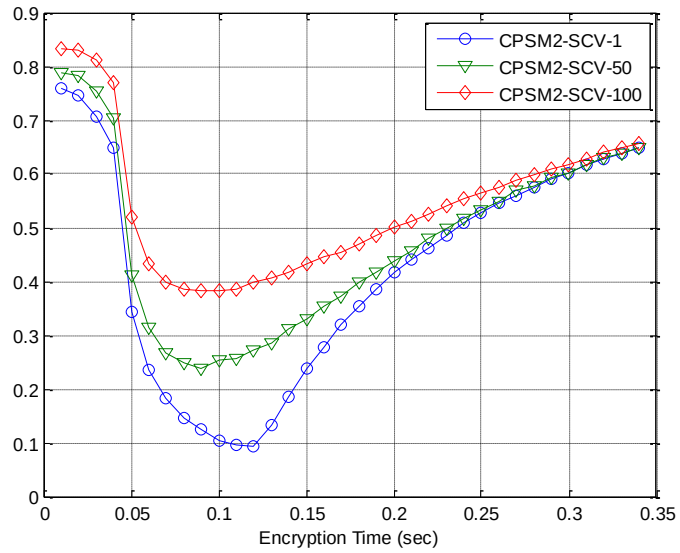


Figure 7-11 $CPSM_2$ for difference SCV vlues of messages interarrival times [1]

7.2.6 Overall Remarks

This framework can model more meaningfully and explicitly the behaviour of security processing and control mechanisms besides capturing the robot's heterogeneity (in terms of the robot architecture and application/task context) in in the near future [1]. Moreover, this framework should enable testing robot's configurations during design development stages of RANETs as well as modifying and tuning existing configurations of RANETs towards enhanced 'optimal' performance and security trade-offs.

The limitation of the framework may include the following issues: there is no explicit formula by which the encryption key lengths can be expressed in terms of the corresponding encryption time. Moreover, the estimation of failure, detection and rekeying times, presented in GSPN security model, needs a wide knowledge of the nature of the modelled system (i.e., its hardware and software) and considered protocol. For the above mentioned reasons, it was not straightforward to validate the results obtained from the model against those of a real system. As a consequence, the overall behaviour of the modelled system was not compared to that of a real system and this is left to be carried out in a future work.

7.3 Summary

In this chapter, a hybrid modelling framework was proposed to support future work on the quantitative analysis of performance vs. security trade-offs in RANETs, where each robotic node was represented by an abstract open hybrid G-GSPN_QN model with multi-class 'On-Off' external arrival process with HoL priorities and associated with CPSMs. The proposed model consisted of four linked sub-models reflecting traffic and (nodal) mobility, security, performance and power consumption with 'intra'-robot component to component communication for mobility control and 'inter'-robot to robot for transmission. More specifically, the model was composed of an open G-GSPN _QN capturing security processing and state-based controls as well as nodal mobility and

power consumption and battery charging and discharging. The G-GSPN sub-model was connected in tandem with an arbitrary QN model with finite capacity channel queues with blocking. Two theoretical case studies from the literature were adapted to illustrate the utility of QN towards modelling intra-robot component to component and inter-robot to robot communications. Furthermore, two extensions of CPSM were suggested for illustration purposes towards facilitating the determination of parameters that may lead to enhanced combined optimisation of performance vs. security trade-off in RANETs.

Chapter 8 Conclusions and Future Work

This chapter includes the main conclusions of the thesis together with future research directions.

8.1 Conclusions

This thesis introduced a quantitative methodology to quantify and predict, under bursty traffic conditions, the performance degradation and associated trade-offs caused by security mechanisms. In this context, an effective quantitative methodology for the analysis of arbitrary QN models and GSPNs through DES was developed based on PEPs in the context of extended applications into performance vs. security trade-offs for high-speed networks with or without infrastructure. In particular, the methodology was employed to carry out investigations on high-speed network routers subject Access Control List (ACL) and also Robotic Ad Hoc Networks (RANETs) with Wired Equivalent Privacy (WEP) and Selective Security (SS) protocols, respectively. The burstiness of traffic was captured by adopting GE-type inter-arrival and service times which also enables predicting the pessimistic 'upper bounds' of the network's performance in the presence of security mechanism. In this regard, Appendices A to G accommodated the implemented simulation algorithms in java for open G-QN models with multiple classes and multiple servers, subject to FCFS and HoL infinite/finite capacity queues with RS-FD blocking and SS, subject to GE and H_2 type inter-arrival and service times. Moreover, a DES algorithm was developed in java for the quantitative analysis of the adopted GSPNs.

More specifically, Chapter 5 presented a high-speed router with Extended-inbound ACL mechanism, where performance degradation of the router was caused due to high-speed incoming traffic in conjunction with ACL security computations making the router a bottleneck in the network. To quantify and predict the trade-off of this degradation, the proposed quantitative methodology employed a suitable open QN model consisting of two queues connected in a tandem configuration corresponding to a security processing node and a transmission forwarding node. PEPs were introduced to the analysis of these two queues and included single or quad-core CPUs with multiple-classes

subject to service with or without priorities (e.g., FCFS or HoL) service disciplines together with space priorities with CBS and PBS buffer management schemes. To this end, performance-related security trade-offs were determined in order to mitigate the adverse effect of security on router's performance. Moreover, RS-FD blocking was employed to reflect the 'Accept-Deny' behaviour of ACL mechanism. Mean response time and PLP were selected as typical performance metrics to assess the improvement in performance and security trade-off. Numerical experiments were carried out, based on DES, in order to establish an 'optimal' balanced trade-off between security and performance towards the design and development of efficient router architectures under bursty traffic conditions.

Moreover, Chapter 6 dealt with the DES analysis of RANETs with WEP and SS protocols (c.f., [46]) in order to achieve, in the presence of limited resources, an 'optimal' compromise between network performance and a tolerable level of security. The focus was on modelling at nodal level of RANETs, as infrastructure-less networks, since the WEP mechanism is performed at each individual robotic node, subject to traffic burstiness and nodal mobility. Therefore, the proposed network model was extended, to reflect the communication of robotic nodes, to be in the form of an open QN model with arbitrary topology comprised from G-queues with dual-core CPU, subject to multiple classes with an infinite capacity queues under FCFS and HoL disciplines. The external arrival traffic flows, which exhibit burstiness, is characterised by an Interrupted Compound Poisson Process (ICPP). The mean marginal end-to-end delay was adopted as a typical performance metric to capture a trade-off balancing performance and security. Numerical DES experiments were carried out according to various scenarios to establish enhanced performance and security trade-offs.

SS was also included in the Gated-QN (G-QN) model with service priority and dual-core CPUs in order to mitigate the adverse effect of security on RANETs performance and establish an 'optimal' performance vs. security trade-off. SS

may achieve great performance vs. security improvements, especially in real-time applications with multimedia information (c.f., [46]). Moreover, including the robot's mobility concept, through G-queue [18 , 59] , within the QN model of a RANET enabling realistic decisions in mitigating the performance of mobile robotic nodes in the presence of security.

The associated numerical experiments for both models in chapters 5 and 6, showed that security improvements achieved by the acquisition of additional hardware and software resources was of 'non-linear nature'. Furthermore, the proposed QN models may clearly assist telecommunications engineers to choose to discriminate against an application that is less sensitive to delay and packet loss, and this will lead to satisfy the required QoS constraints.

Finally, Chapter 7 proposed an enhanced quantitative methodology in the form of an advanced hybrid framework for capturing 'optimal' performance vs. security trade-offs for each node of a RANET by taking more explicitly into consideration security control and battery life. Specifically, each robotic node was represented by a hybrid Gated GSPN (G-GSPN) and a QN model.

In this context, the G-GSPN included bursty multiple class traffic flows, nodal mobility, security processing and control whilst the QN model has, generally, an arbitrary configuration with finite capacity channel queues to reflect 'intra' robot(component-to-component) communication and 'inter' robot-to-robot transmissions.

In particular, two theoretical QNs models were adapted from the literature [21 , 22 , 23] on secure robot to illustrate the utility of a QN towards reflecting 'intra' and 'inter' robot communications. Finally, two examples on extending CPSMs, based on the CPSM proposed by Wolter and Reinecke [13], were proposed towards the determination of an 'optimal' performance and security trade-off.

To summarise, the potential applicability of the hybrid framework may include: i) Modelling more meaningfully and explicitly the behaviour of security processing and control mechanisms; ii) Capturing RANET's heterogeneity (in terms of the robot architecture and application/task context) in the near future (c.f. [1]) and

iii) Testing, modifying and tuning the configurations of RANETs during design and development stages towards ‘optimal’ performance and security trade-offs.

8.2 Recommendations for Future Work

Possible extensions of the work include the following research themes and associated applications in RANETs:

1. Developing new protocols in order to optimise different CPSMs for diverse RANETs applications under bursty and correlated traffic flows [24]. Possible correlated traffic flows are the Batch Markovian Arrival Process (BMAP) and Batch Renewal Process (BRP). Note that the BMAP is a generalisation of Poisson process that allows arrivals of correlated batch sizes, in addition to dependent non-exponentially distributed inter-arrival times (c.f., [121]). On the other hand, a BRP facilitates the investigation of the impact of correlation on network’s performance independently of any other traffic characteristics and it is completely defined by sets of counts and intervals correlations by means of Index of Dispersion for Counts (IDCs) and it is defined as the variance in the number of arrivals in an interval of time *t* divided by the mean number of arrivals in time *t* and Index of Dispersion for Intervals (IDIs) and it is defined as the variance of n intervals between n+1 individual arrivals divided by the squared mean of this interval (c.f.,[122]). BMAP and BRP can be constructed with the same IDCs and IDIs (c.f., [123]) and be used to obtain numerically optimistic and pessimistic CPSMs, respectively.

2. Applying the ME principle and a queue-by-queue decomposition algorithm (as proposed in [16 , 20 , 87] to investigate performance-related security of routers and RANET. Such an approach will facilitate the design and evaluation of optimal trade-offs between performance and security Furthermore, the coordination and implementation of a more globally-related standardisation process (c.f., European Telecommunications Standards Institute (ETSI), Institute of Electrical and Electronics Engineers (IEEE), etc.) for networked mobile wireless robotics is recommended, thereby

guaranteeing high performance levels in the presence of efficient security mechanisms. Exploiting ME principle could help in overcoming potential state space explosion caused by increased the network size and the inclusion of multiple classes and blocking mechanisms;

3. Designing and developing optimal broadcasting/multicasting algorithms to achieve performance gains in RANETs, such as those based on tree and cluster methods proposed by Mkwawa and Kouvatsos (c.f., [124])). This poses challenging problems because of the “variable and unpredictable characteristics of RANET’s medium as well as the fluctuation of signal strength and propagation with respect to time and environment” (c.f.,[54]);

4. Exploiting the synergy and operational cognitive similarities between RANETs and Cognitive Radio Mobile Wireless Ad Hoc Networks (CRAHNs), will be of interest since RANETs may employ Cognitive Radio (CR) to extend the cognitive-type functionalities and attributes of robotic nodes, such as new techniques for cooperative heterogeneous network architectures, dynamic spectrum access, security mechanisms etc. Conversely, CR-based RANETs may “form suitable intelligent test beds for motivating, informing, assessing, validating, predicting and verifying concepts and mechanisms for CRAHNs” (c.f., [28 , 54 , 69 , 125]);

5. Extending the GSPN security model proposed by Wolter and Reinecke [13], to include the protection (or reduction) of information leakage when the system is non-secure. This model can then be associated with more advanced security protocols like IDS for GCS proposed by Cho in [15] by utilising the hybrid GSPN and QN framework;

6. Exploiting the library of security mechanisms proposed by Cortellessa and Trubiani [41], which includes the implementation of a GSPN model that is applicable to several types of security services, such as access control and encryption, which may be used for representing security operations under the auspices of the proposed hybrid G-GSPN_QN framework;

7. Implementing the proposed RANET hybrid G-GSPN_QN model in the context of autonomous robots and considering multi-robot single tele-operator and multi-robot multi tele-operator [117] instead of a single robot. Moreover, the framework can be integrated with the architecture proposed by Redi and Bers in[126] for autonomous robots operations including routing protocols, internal robot communications and data forwarding.

8. Finally, investigating further the credibility of Fuzzy Petri Nets (FPNs) [127] and Coloured Fuzzy Petri Nets (CFPN) [128] models in the context of routing protocols for RANETs. These models have been successfully employed to investigate MANETs with incomplete information about state and time (c.f., [128 , 129 , 130]). Note that in FPNs, one or more of the PN components can be fuzzy (i.e., the information they convey may be ‘uncertain and incomplete’ [129]).

References

[1] D. D. Kouvatsos, G. M. A. Miskeen, and E. Habibzadeh, "Performance Modelling and Evaluation of Secure Dynamic Group Communication Systems in RANETs," 2013.

[2] D. D. Chowdhury, *High-Seed LAN Technology Handbook*: Springer, 2000, pp. 429-435.

[3] P. Jungck and S. S. Yshim, "Issues in high-speed Internet security," *IEEE Computer Society*, vol. 37, no.7, pp. 22-28, 2004.

[4] W. Stallings, *High-Speed Networks and Internets: Performance and Quality of Service*, 2nd ed. India: Pearson Education-Prentice Hall, 2002.

[5] J. Velissarios and R. Santarossa, "Practical security issues with high-speed networks," *Journal of High-Speed Networks*, vol. 8, no.4, pp. 311-324, 1999.

[6] V. Zorkadis, "Security versus performance requirements in data communication systems," *In Proc.* of the 3rd European Symposium on Research in Computer Security Computer Security (ESORICS), vol. 875, pp. 19-30, 1994.

[7] N. M. K. Chowdhury, "Literature Review: adaptive analysis of high-speed router performance in packet-switched networks," 2007, pp. 1-10. Available:http://www. mosharaf.com/wp-content/uploads/nmmkchow-adaptive-survey-spring07.pdf. [Accessed : 8 Feb. 2010].

[8] S. Molnar, Maricza, I., Maricza, I., Daniels, T., Färber, J., Frater, M., et.al., "Source characterization in broadband networks," Mid-term seminar interim report on source characterization , Vilamoura, Portugal, COST 257, 1999.

[9] S. Pillalamarri and S. Ghosh, "High-speed networks: definition and fundamental attributes," *Computer Communications*, vol. 28, no. 8, pp. 956-966, 2005. Avaiable: http://www.science direct.com /science /article/pii/S0140366404002671. [Accessed: 4 Jun. 2010].

[10] G. Lehembre, "Wi-Fi Security -WEP, WPA and WPA2," Report, 2005. Avaiable: www.hsc.fr/ressources/articles/ha kin9_wifi/hakin9wifiEN.pdf. [Accessed: 27 May 2012].

[11] R. Yonglin, A. Boukerche, and L. Mokdad, "Performance analysis of a selective encryption algorithm for wireless ad hoc networks," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, 2011, pp. 1038-1043. Avaiable:http://ieeexplore.ieee.org /xpls/abs _all.jsp?arnumber=5779278&tag=1. [Accessed: 25 Aug. 2011].

[12] D. D. Kouvatsos, "A maximum entropy analysis of the G/G/1 queue at equilibrium," *The Journal of the Operational Research Society*, vol. 39, no. 2, pp. 183-200, 1988.

[13] K. Wolter and P. Reinecke, "Performance and security trade-off," in *Formal Methods for Quantitative Aspects of Programming Languages*, *Computer sience Lecture Notes*, vol. 6154, A. Aldini, M. Bernardo, A. Di Pierro, and H. Wiklicky, Eds. Berlin, Heidelberg: Springer 2010, pp. 135-167.

[14] M. Saleh and I. Al Khatib, "Performance of secure ad hoc sensor networks utilizing IEEE802. 11b WEP," in *Proc. of Systems Communications*, Montreal, Que., Canada, 2005, pp. 68 - 72.

[15] J. H. Cho, R. Chen, and P. G. Feng, "Performance analysis of dynamic group communication systems with intrusion detection integrated with batch rekeying in mobile ad hoc networks," in *Proc. of 22nd International Conference on Advanced Information Networking and Applications Workshops (AINAW)*, Okinawa, 2008, pp. 644-649.

[16] D. Kouvatsos and I. Awan, "Entropy maximisation and open queueing networks with priorities and blocking," *Performance Evaluation*, vol. 51, no. 2, pp. 191-227, 2003.

[17] S. S. Yau, Y. Nong, H. S. Sarjoughian, H. Dazhi, A. Roontiva, M. Baydogan, and M. A. Muqsith, "Toward development of adaptive service-based software systems," *IEEE Trans. on Services Computing*, vol. 2, pp. 247-260, 2009. Avaiable: http://ieeexplore.ieee.org/xpls/abs _all.jsp?arnumber= 5156 491& tag=1. [Accessed: 6 May 2012].

[18] H. Bhatia, R. Lening, S. Srivastava, and V. Sunitha, "Application of QNA to analyze the queueing network mobility model of MANET," Technical Report, Dhirubhai Ambanil institute of Information & Communication Technology (DAIICT), Gandhinagar, India, 2007. Avaiable:http://www.sci .utah.edu/~hbhatia/docs/ Harsh Bhatia_BTP.pdf. [Accessed: 3 Jun. 2011].

[19] G. Bolch, S. Greiner, H. de Meer, and K. S. Trivedi, *Queueing networks and Markov chains: modeling and performance evaluation with computer science applications*. Hoboken, New Jersey: John Wiley & Sons, Inc, 2006.

[20] D. D. Kouvatsos, "Entropy maximisation and queueing network models," *Annals of Operations Research*, vol. 48, no. 1, pp. 63-126, 1994.

[21] B. B. Luu, B. J. O'Brien, D. G. Baran, and R. L. Hardy, "A soldier-robot ad hoc network," in *Proc. of 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom)*, White Plains, NY, 2007, pp. 558-563. Avaiable: http://ieeexplore .ieee.org/xpl/article Details.jsp?arnumber=4144898. [Accessed:23 Jun. 2013].

[22] R. Rocha, J. Dias, and A. Carvalho, "Cooperative multi-robot systems: a study of vision-based 3-D mapping using information theory," *Robotics and Autonomous Systems*, vol. 53, no. 3, pp. 282-311, 2005.

[23] F. Zeiger, N. Kraemer, M. Sauer, and K. Schilling, "Challenges in realizing ad-hoc networks based on wireless LAN with mobile robots," in *Proc. of 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops (WiOPT)*, Berlin, 2008, pp. 632-639. Avaiable: http://ieeexplore. ieee.org/stamp/ stamp.jsp?arnumber=04586151. [Accessed: 12 Jun. 2013].

[24] Z. Cui and A. A. Nilsson, "The impact of correlation on delay performance of high speed networks," in *Proc. of the 26th Southeastern Symposium on System Theory*, Athens, OH, 1994, pp. 371-374. Avaiable: http://ieeexplore.ieee.org/ xpls/abs_all.jsp? arnumber=287850. [Accessed: 20 Nov. 2012].

[25] E. A. Khalil, "Comparative performance of high speed networks carrying multimedia," *International Journal of Engineering Sciences & Emerging Technologies (IJESET)*, vol. 3, no. 1, pp. 9-21, 2012.

[26] F. K. James and W. R. Keith, *Computer Networking: A top-down Approach Featuring the Internet*, 3 ed. Boston, Massachusetts: Addison-Wesley, 2004.

[27] A. Alabady, "Design and implementation of a network security model for cooperative network," *International Arab Journal of e-Technology*, vol. 1, no. 2, pp. 26-36, 2009.

[28] D. D. Kouvatsos, "Performance and security trade-offs in robotic mobile wireless ad hoc networks (RANETs)", PP Presentation of Invited Talk in the14th Strategic Workshop (SW'12) on Wireless Robotics - Research and Standardisation: Dronninglund Castle, Slotsgade 8, 9330, Denmark, 2012.

[29] Z. Wang, L. Liu, and M. C. Zhou, "Protocols and applications of ad-hoc robot wireless communication networks: an overview," *The International Journal of Intelligent Control Systems*, vol. 10, no. 4, pp. 296-303, 2005.

[30] W. Vandenberghe, I. Moerman, and P. Demeester, "Adoption of vehicular ad hoc networking protocols by networked robots," *Wireless Personal Communications*, vol. 64, no. 3, pp. 489-522, 2012.

[31] M. P. Groover, 2008. Automation, Production Systems, and Computer-Integrated Manufacturing, [Online eBook]. Available: http://www.nuigalway.ie/staff-sites/david_osullivan /documents/ unit_6_ industrial_robotics.pdf. [Accessed: 10 Mar. 2013].

[32] K. Virk, K. Hansen, and J. Madsen, "System-level modeling of wireless integrated sensor networks," in *International Proc. of Symposium System-on-Chip*, Tampere, 2005, pp. 179-182. Available: ttp://ieeexplore.ieee.org/xpls/abs_all. jsp? Arnumber =1595672. [Accessed: 10 Dec. 2012].

[33] S. K. Parmar, 2007. Information Resource Guide Computer, Internet and Network Systems Security: An Introduction to Security. [Online eBook]. Available: http://cite seerx.ist.psu.edu /viewdoc/summary?doi=10.1.1.153.5669 [Accessed: 3 Feb. 2010].

[34] A. O. Allen, *Probability, statistics, and queueing theory: with computer science applications*. London, UK: Academic Press, 1990.

[35] R. Asokan and A. Natarajan, S. Adibi, Jain, R., Parekh, R., Tofighbakhsh, M. "Quality of service (QoS) routing in mobile ad Hoc networks," in *Quality of Service Architectures for Wireless Networks: Performance Metrics and Management*, S. Adibi, R. Jain, R. Parekh, M. Tofighbakhsh, , Eds.: Information Science Reference, 2010, pp. 464-496.

[36] F. Bertocchi, P. Bergamo, G. Mazzini, and M. Zorzi, "MAC and routing solution for energy saving in ad hoc networks: distributed power control," in *Proc. of the 2003 Joint Conference of the 4th International Conference on Information, Communications and Signal Processing*, 2003, vol. 2, pp. 1061-1065. Avaiable: http://ieeexplore. ieee.org /xpls/abs_all.jsp?arnumber =1292622 &tag =1. [Accessed: 8 Jul. 2011].

[37] D. Vaman and L. Qian, "Cognitive radio mixed sensor and mobile ad hoc networks (SMANET) for dual use applications," in *Proc. of IEEE International Conference on Systems, Man and Cybernetics (SMC)*, Singapore, 2008, pp. 3304-3310. Available: http://ieeexplore.ieee. org/xpls/abs_all.jsp?arnumber =4811806 &tag=1. [Accessed: 20 Nov. 2011].

[38] M. Maleki, K. Dantu, and M. Pedram, "Power-aware source routing protocol for mobile ad hoc networks," in *Proc. of the 2002 International Symposium on Low Power Electronics and Design (ISLPED)*, 2002, pp. 72-75. Available: http://ieeexplore .ieee.org/stamp /stamp.jsp?tp=& arn umber=1029549. [Accessed: 1 Nov. 2011].

[39] K. T. Fung, *Network Security Technologies*, 2nd ed. Boca Raton, Florida: CRC Press, 2005.

[40] E. Maiwald, *Network security: A Beginner's Guide*. Osborne, Kansas: McGraw-Hill Professional, 2001.

[41] V. Cortellessa and C. Trubiani, "Towards a library of composable models to estimate the performance of security solutions," in *Proc. of the 7th international workshop on Software and Performance*, Princeton, NJ, USA, 2008, pp. 145-156. Available: http://dl.acm.org/ citation. Cfm ?id=1383579. [Accessed : 29 Sep. 2012].

[42] F. C. Freiling, "Introduction to security metrics," *Dependability Metrics*, vol. 4909, pp. 129-132, 2008.

[43] B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "Modeling and quantification of security attributes of software systems," in *Proc. of the International Conference on Dependable Systems and Networks,* Washington, USA,2002, pp. 505-514. Available: http://ieeexplore.ieee.org/stamp /stamp.jsp?tp= &arnum ber=1028941. [Accessed : 26 Jan. 2013].

[44] R. M. Savola and H. Abie, "On-line and off-line security measurement framework for mobile ad hoc networks," *Journal of Networks*, vol. 4, no. 7, pp. 565-579, 2009.

[45] S. S. Gokhale and K. S. Trivedi, "Analytical modeling," in *Encyclopedia of Distributed Systems*: Kluwer Academic Publishers, 1998.

[46] S. S. Yau, Y. Yin, and H. G. An, "An adaptive trade-off model for service performance and security in service-based systems," in *Proc. of IEEE International Conference on Web Services (ICWS)*, Los Angeles, CA, 2009, pp. 287-294. Avaiable: http://ieeexplore. ieee.org/xpls/abs _all.jsp? arnu mber=5175835&tag=1. [Accessed: 5 Apr. 2012].

[47] R. Stedman, "Access control lists ", Lecture Notes, Department of Electrical Engineering and computer science, University of Bremen, Bremen, 2010. Avaialble: http://www.weblearn.hs-bremen.de/lehrenden/sethmann /Network ing/ Lecture/ Networking_ACLs.pdf. [Accessed: 20 Apr. 2010].

[48] S. Antoniou. Cisco IOS Access Control Lists (ACLs). [Online]. Available: http://www. trainsignal.com/blog/cisco-access-lists. [Accessed: Dec. 2012].

[49] R. Deal, *CCNA Cisco Certified Network Associate Study Guide (Exam 640-802)*: McGraw-Hill, 2008.

[50] R. Kayne. What is a dual core processor. Available: http://www.wisegeek.com/what-is-a-dual-core- processor.htm. [Accessed: 4 Feb. 2010].

[51] Q. M. Plummer. Dual core processors. Available: http://www.ehow.com/dual-core-processors/. [Accessed: 5 Feb. 2010].

[52] Wi-Fi. Alliance, "Deploying Wi-Fi protected access (WPA ™) and WPA2 ™ in the enterprise", White Paper 2005. Available: http://www.wi-fi.org/files/wp_9_ WPA-WPA2%20Implementation_2-27-05.pdf. [Accessed: 17 Oct. 2011].

[53] H. cooper, "Teletraffic theory and engineering," in *Encyclopedia of Telecomunications*, vol. 16. New York, USA: Marcel Dekker, Inc., 1998, pp. 453-483.Available: http://www.cse.fau.edu/~bob/ publications/ cooper .heyman- previous. pdf. [Accessed: 17 Oct. 2011].

[54] D. D. Kouvatsos and G. M. A. Miskeen, "Networked mobile wireless robotics," Technical Report, Networks and Performance Engineering (NetPEn) Research Group, Informatics Research Institute,University of Bradford, Bradford, UK, DDK-NetPEn 15-02-11, 2011.

[55] Q. Wang, "Traffic analysis and modeling in wireless sensor networks and their applications on network optimization and anomaly detection," *Network Protocols and Algorithms*, vol. 2, no. 1, pp. 74-92, 2010.

[56] Q. Wang, "Traffic analysis, modelling and their applications in energy-constrained wireless sensor networks on network optimization and anomaly detection," PhD thesis, Department of Information Technology and Media, Sweden Mid University, Sundsvall, Sweden, 2010.

[57] F. Gebali, *Analysis of Computer and Communication Networks*: Springer, 2008.

[58] H. Okamura, Y. Kamahara, and T. Dohi, "Estimating Markov-modulated compound Poisson processes," in *Proc. of the 2nd International Conference on Performance Evaluation Methodologies and Tools (Valuetools'07), ACM International Conference Proceeding Series*, 2007, vol. 321, pp. 1-8. Avaialbe: http://dl.acm.org/citation.cfm?id =1345299. [Accessed: 14 May 2011].

[59] H. Bhatia, R. Lenin, A. Munjal, S. Ramaswamy, and S. Srivastava, "A queuing-theoretic framework for modeling and analysis of mobility in WSNs*," in Proc. of the 8th Workshop on Performance Metrics for Intelligent Systems (PerMIS),* 2008, pp. 248-253. Avaiable: http://dl.acm.org/citation.cfm?id=1774713. [Accessed: 19 Dec. 2010].

[60] K. Sigman, "Poisson processes and compound (batch) Poisson processes." Lecture Notes. Columbia University, USA, 2007. Avaialbe: http://www.columbia.edu/ ~ks20/4703 -Sigman/4703-07-Notes-PP-NSPP.pdf. [Accessed: 20 Jun. 2011].

[61] A. Nogueira and R. Valadas, "Analysing the versatility of the 2-MMPP traffic model," in *Proc. of the 2nd International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP)*, Bournemouth, UK, 2001, pp. 261–266.Avaialbe :http://www.av.it.pt/rv/ Papers /csndsp00 _mmpp.pdf. [Accessed: 14 May 2011].

[62] A. Nogueira, P. Salvador, and R. Valadas, "Fitting algorithms for MMPP ATM traffic models," in *Proc. of the Broadband Access Conference*, 1999, pp. 167-174. Avaialbe: http://www.av.it.pt/rv/Papers/bac99_ mmpp.pdf. [Accessed: 15 May 2011].

[63] P. K. Suri and K. Taneja, "Integrated queuing based energy-aware computing in MANET" *International Journal of Computer Science and Information Security*, vol. 8, no. 3, pp. 7-10, 2010.

[64] A. M. H. Ardawi, "Performance modeling and evaluation of robotic ad hoc mobile wireless networks (RMWNs)," MSc Thesis, Department of Computing, University of Bradford, UK, 2010.

[65] G. Miskeen, D. D. Kouvatsos, and M. Akhlaq, "Performance and security trade-off for routers in high speed networks," in *Proc. of the 26th UK Performance Engineering Workshop*, S.Hammond, S. Jarvis , M. Leeke, Eds.,University of Warwick, 2010, pp. 119-128

[66] V. Jain and M. Jain, "Queuing network model for link and path availability of ad hoc networks," in *Proc. of IFIP International Conference on Wireless and Optical Communications Networks*, 2006, pp1-5. Avaialbe:http://ieeexplore. ieee.org/ stamp/ stamp.jsp?tp=&arnumber =1666563. [Accessed: 20 Jan. 2011].

[67] V. Jain, R. B. Lenin, and S. Srivastava, "Modeling MANETs using queueing networks," in *Proc. of National Conference of Communications (NCC)*, 2007, pp. 1-5. Avaialbe: www.ncc.org.in/down load .php?f=NCC2007/1.3.2.pdf .[Accessed: 20 Jan. 2011].

[68] S. Shah, R. Lenin, S. Ramaswamy, and S. Srivastava, "Modeling and analysis of mobility in MANETs for distributed applications," *Distributed Computing and Internet Technology*, Lecture Notes in Computer Science, vol. 5375, pp. 100-108, 2009.

[69] D. D. Kouvatsos and G. M. A. Miskeen, "Performance related security modelling and evaluation of RANETs," *Wireless Personal Communications*, vol. 64, no. 3, pp. 523-546, 2012.

[70] Y. Xu and X. Xie, "Modeling and analysis of security protocols using colored Petri nets," *Journal of Computers*, vol. 6, no. 1, pp. 19-27, 2011.

[71] A. Al-Khatib, "Performance analysis of wireless LAN access points," PhD thesis, Department of Microelectronics and Information Technology, Royal Institute of Technology, Stockholm, Sweden, 2003.

[72] C. Zhang, "Ad hoc network security and modeling with stochastic Petri nets," PhD thesis, Department of Electrical and Computer Engineering, New Jersey Institute of Technology, NJ, 2005.

[73] C. Zhang and M. Zhou, "A stochastic Petri net-approach to modeling and analysis of ad hoc network," in *Proc. of International Conference on Information Technology: Research and Education (ITRE)*, 2003, pp. 152-156. Avaiable: http://ieeexplore .ieee.org/ xpls/abs_all.jsp?arnumber=1270592&tag=1. [Accessed: 4 Apr. 2012].

[74] D. D. Kouvatsos and G. Miskeen, "Performance related security trade-off for routers in high -speed networks," in *Proc. of the 27th UK Performance Engineering Workshop (UKPEW)*, I.U. Awan,G. Min, R. Osman, Eds., 2011, pp. 303-325.

[75] W. Y. Zibideh and M. M. Matalgah, "An optimized encryption framework based on the modified-DES algorithm: a trade-off between security and throughput in wireless channels," in *Radio and Wireless Symposium (RWS)*, Santa Clara, CA , 2012, pp. 419-422. Avaiable: http://ieee xplore .ieee.org /xpls/abs_ all.jsp?arnumber=6175391. [Accessed: 28 May 2012].

[76] R. Curtmola, J. Dong, and C. Nita-Rotaru, "Trade-offs between security and communication performance in wireless mesh networks," in *Proc. of 2010 IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM)*, Montreal, QC, Canada, 2010, pp. 1-6. Avaialbe: http:// ieeexplore.ieee .org/stamp/stamp.jsp?tp=&arnumber=5535005. [Accessed: 20 Apr. 2012].

[77] M. A. Haleem, C. N. Mathur, R. Chandramouli, and K. P. Subbalakshmi, "Opportunistic encryption: a trade-off between security and throughput in wireless networks," *IEEE Trans. on Dependable and Secure Computing*, vol. 4, no. 4, pp. 313-324, 2007.

[78] Z. Wente and C. Mo-Yuen, "A trade-off model for performance and security in secured networked control systems," in *IEEE International Symposium on Industrial Electronics (ISIE)*, Gdansk, 2011, pp. 1997-2002. Avaiable: http://ieeexplore.ieee. org/stamp/stamp.jsp? tp=&arnumber =598 4466. [Accessed: 5 Nov. 2012].

[79] Z. Wente and C. Mo-Yuen, "Optimal trade-off between performance and security in networked control systems based on coevolutionary algorithms," *IEEE Trans. on Industrial Electronics*, vol. 59, no. 7, pp. 3016-3025, 2012.

[80] M. Becker and H. Szczerbicka, "PNiQ: integration of queuing networks in generalised stochastic Petri nets," *IEE Proc. on Software*, vol. 146, no. 1, pp. 27-32, 1999.

[81] S. Kounev and A. Buchmann, "SimQPN- a tool and methodology for analyzing queueing Petri net models by means of simulation," *Performance Evaluation*, vol. 63, no. 4, pp.364-394, 2006.

[82] S. Kounev, "Performance modeling and evaluation of distributed component-based systems using queueing petri nets," *IEEE Trans. on Software Engineering*, vol. 32, pp. 486-502, 2006.

[83] S. Kounev and A. Buchmann, V. Kordic "On the use of queueing petri nets for modeling and performance analysis of distributed systems," in *PetriNet, Theory and Application*, V. Kordic, Ed. Vienna, Austria, 2008, pp. 149-178.

[84] D. D. Kouvatsos and I. M. Mkwawa, "Multicast communication in grid computing networks with background traffic," *IEE Proceedings of Software*, vol. 150, no. 4, pp. 257-264, 2003.

[85] M. Gribaudo and M. Sereno, "GSPN semantics for queueing networks with blocking," in *Proc. of the 7th International Workshop on Petri Nets and Performance Models*, Saint Malo, 1997, pp. 26-35. Avaiable: http://ieee xplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=595534. [Accessed: 11 Apr. 2012].

[86] G. Balbo, S. C. Bruell, and S. Ghanta, "Combining queueing networks and generalized stochastic petri nets for the solution of complex models of system behavior," *IEEE Trans. on Computers*, vol. 37, no. 10, pp. 1251-1268, 1988.

[87] D. D. Kouvatsos, J. S. Alanazi, and K. Smith, "A Unified ME algorithm for arbitrary open QNMs with mixed blocking mechanisms," *Numerical Algebra, Control and Optimization (NACO)*, vol. 1, no. 4, pp. 781-816, 2011.

[88] A. Munjal, "Modeling MANETs using queueing networks," Master thesis abstract, Dhirubhai Ambani Institute of Information & Communication Technology, (DAIICT), Gandhinagar, INDIA, 2007. Avaiable: http://magnet. daiict. ac.in/Theses /AartiMunjalMTech2005_Thesis Abstract.pdf. [Accessed: 17 Dec. 2011].

[89] G. Balbo and G. Chiola, "Stochastic Petri net simulation," in *Proc. of the 21st conference on Winter simulation (WSC)*, Washington, DC–Piscataway, NJ, 1989, pp. 266-276. Avaiable: http://dl.acm.org/citation.cfm?id=76772. [Accessed: 17 Dec. 2011].

[90] S. Guiasu, "Maximum Entropy Condition in Queueing Theory," *The Journal of the Operational Research Society*, vol. 37, no. 3, pp. 293-301, 1986.

[91] M. A. Marsan, G. Rozenberg "Stochastic Petri nets: an elementary introduction," in *Advances in Petri Nets,* vol. 424, G. Rozenberg, Ed.: Springer Verlag, 1990, pp. 1-29.

[92] M. A. Marsan, G. Balbo, G. Chiola, G. Conte, S. Donatelli, and G. Franceschinis, "An introduction to generalized stochastic Petri nets," *Microelectronics Reliability*, vol. 31,no. 4, pp. 699-725, 1991.

[93] M. A. Marsan, A. Bobio, and S. Donatell, W. Reisig and G. Rozenberg "Petri nets in performance analysis: an introduction," in *Lectures on Petri Nets I: Basic Models*, vol. 1491, W. Reisig and G. Rozenberg, Eds. Berlin, Germany.: Springer-Verlag, 1998, pp. 211–256.

[94] G. Balbo, "Stochastic Petri nets: Accomplishments and open problems," in *Proc*. of *Computer Performance and Dependability Symposium,* 1995, pp. 51-60. http://ieeexplore.ieee.org/xpls/abs_all.jsp? arnumber=395817. [Access: 10-4-2013].

[95] F. Bause, "Queueing Petri nets- a formalism for the combined qualitative and quantitative analysis of systems," in *Proc. of the 5th International Workshop on Petri Nets and Performance Models*, Toulouse, France, 1993, pp. 14-23. Avaiable: http:// ieeexplore.ieee.org/stamp/ stamp.jsp?tp =&arnumber=393439. [Accessed: 4 May 2012].

[96] M. Becker and H. Szczerbicka, "Integration of multi-class queueing networks in generalized stochastic Petri nets," in *Proc. of IEEE International Conference on Systems, Man, and Cybernetics*, 2001, vol. 2, pp. 1137-1142. Avaiable: http://ieeexplore .ieee.org/stamp /stamp. jsp? tp=&arnumber =1309629. [Accessed: 18 Jun. 2012].

[97] H. Szczerbicka, "A combined queueing network and stochastic Petri net approach for evaluating the performability of fault-tolerant computer systems," *Performance Evaluation*, vol. 14, pp. 217-226, 1992.

[98] Z. Cao, F. Qiao, and Q. Wu, "Queueing generalized stochastic colored timed Petri nets based approach to modeling for semiconductor wafer fabrication," in *Proc. of IEEE International Conference on Control and Automation*, Guangzhou, China, 2007, pp. 2834-2838. Avaiable: http://ieeexplore. ieee.org/stamp/stamp.jsp?tp= &arnumber =4376879. [Accessed: 12 Jul. 2012].

[99] M. Becker and H. Szczerbicka, "Combined modeling with generlized stochastic Petri nets Including queueing nets," in *Proc. of 14th UK Computer and Telecommunications Performance and Engineering Workshop*, 1998, pp. 48-62.www.sim.uni-hannover.de/ ~xmb/Postscript/ pew sent.ps. [Accessed: 12 Jul. 2012].

[100] F. Bause and P. Buchholz, "Queueing petri nets with product-form solution," *Performance Evaluation*, vol. 32, no. 4, pp. 265-299, 1998.

[101] K. M. Chandy, U. Herzog, and L. Woo, "Parametric analysis of queuing networks," *IBM Journal of Research and Development*, vol. 19, no. 1, pp. 36-42, 1975.

[102] H. Szczerbicka and P. Ziegler, "Simulation with active objects: an approach to combined modelling," *Simulation Practice and Theory*, vol. 1, no. 6, pp. 267–281, 1994.

[103] M. Saleh and I. Al Khatib, "Throughput analysis of WEP security in ad hoc sensor networks," in *Proc. of 2nd International Conference on Innovations in Information Technology (IIT)*, Montreal, Que., Canada, 2005, pp. 26-28. Available:http://www.it-innovations.ae/iit005/proceedings /articles/a_3 _iit05 _ saleh_ khatib.pdf. [Accessed: 16 Sep. 2011].

[104] N. Mir, *Computer Communication Networks*: Prentice Hall, 2007.

[105] A. Law and D. Kelton, *Simulation Modeling and Analysis*, 3rd edition ed: McGraw-Hill, 2000.

[106] D. Wischik, "Buffer requirements for high-speed routers," in *Proc. of the 31st European Conference on Optical Communication (ECOC)*, 2005, vol. 5, pp. 23 – 26. Available: http://ieee xplore.ieee.org/xpls/abs _all.jsp?arnumbe r=1584319.[Accessed: 5 Apr. 2010].

[107] W. Kai, L. Chuang, and L. Fangqin, "Quality of protection with performance analysis in IP multimedia subsystem," in *Proc. of the 8th EEE/ACIS International Conference on Computer and Information Science (ICIS)*, Shanghai, China, 2009, pp. 234-239. Available:http://ieeexplore.ieee .org/xpls/abs_all. jsp?arnumber=5223068. [Accessed: 15 Jul. 2012].

[108] D. D. Kouvatsos, P. Georgatsos, P. Tomaras, and N. Xenios, "Probabilistic GE-type Algebra for Single Server GE-type Queues," Technical Report, Department of Computing, University of Bradford, Bradford, UK 1989.

[109] S. L. Kim, W. Burgard, and D. E. Kim, "Wireless communications in networked robotics," *IEEE Wireless Communications,* vol. 16, no. 1, pp. 4-5, 2009.

[110] D. D. Kouvatsos, " Performance modeling and evaluation of RANETs," Presented at 1st ETSI Workshop on Networked Mobile Wireless Robotics. [presentation]. Available: http://workshop .etsi.org/2010/201010_ Network ed MobileWirelessRobotics/ 06% 20 Kouvatsos %202010-10-08%20Networked%20Robots.pdf .

[111] E. Barka and M. Boulmalf, "On the impact of security on the performance of WLANs," *Journal of Communications*, vol. 2, no. 4, pp. 10-17, 2007.

[112] G. M. A. Miskeen, " A Portfolio of simulation programs in java for the analysis of arbitrary open G-QNMs," University of Bradford, UK, Technical Report TR- MGMA-5, 2011.

[113] F. Bause, "QN+ PN= QPN"-combining queueing networks and Petri nets," Technical Report, Department of Computer Science, University of Dortmund, Germany, 461, 1993. Available: http://citeseerx.ist.psu.edu/viewdoc /summary ?doi=10.1.1.46.9867. [Accessed: 10 Mar. 2012].

[114] Y. Mei, Y.-H. Lu, Y. C. Hu, and C. G. Lee, "A case study of mobile robot's energy consumption and conservation techniques," in *Proc. of 12th International Conference on*

Advanced Robotics (ICAR), *Seattle, WA,* 2005, pp. 492-497. Available: http://ieee xplore.ieee*. org/xpls/abs_all.jsp? arnumber=1507454.* [Accessed: 28 May 2013].

[115] M. Hu and S. Zou, "Analysis of cryptographic protocol about wireless LAN base on Petri net," in *Proc. of International Conference on Computer Application and System Modeling (ICCASM)*, Taiyuan, 2010, vol. 8, pp. 267-269. Available: http://ieeexplore. ieee.org/xpls/abs_all.jsp?arnumbe r=5619304 &tag=1. [Access ed:10 August 2012].

[116] A. F. Winfield, L. E. Parker, G. Bekey, and J. Barhen, "Distributed sensing and data collection via broken ad hoc wireless connected networks of mobile robots," in *Distributed Autonomous Robotic Systems,* vol. 4: Springer-Verlag 2000, pp. 273-282.

[117] F. Gao and M. Cummings, "Using discrete event simulation to model multi-robot multi-operator teamwork," in *Proc. of the Human Factors and Ergonomics Society 56th Annual Meeting*, 2012, vol. 56, no. 1, pp. 2093-2097. Available:http://pro.sagepub.com/ content/56/1/2093.short. [Accessed :5 Jul. 2013].

[118] G. Balbo, M. Beccuti, M. De Pierro, and G. Franceschinis, "First passage time computation in tagged GSPNs with queue places," *The Computer Journal*, vol. 54, no. 5, pp. 653-673, 2011.

[119] S. Balsamo and A. Marin, "On representing multiclass M/M/k queue by generalized stochastic Petri net," in *Proc. of ECMS/ASMTA-2007 Conference*, Prague, Czech Republic. 2007, pp. 121-128. Available: http://citeseerx.ist.psu. edu/viewdoc/summary ?doi=10.1.1.181.1136. [Accessed: 5 Jun. 2013].

[120] J. H. Cho, A. Swami, and I. R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1001-1012, 2012.

[121] D. M. Lucantoni, L. Donatiello and R. Nelson "The BMAP/G/1 queue: a tutorial," in *Models and Techniques for Performance Evaluation of Computer and Communication Systems Joint Tutorial Papers of Performance '93 and Sigmetrics '93*, vol. 729, L. Donatiello and R. Nelson, Eds. London, U.K: Springer Berlin Heidelberg, 1993, pp. 330-358.

[122] R. Gusella, "Characterizing the variability of arrival processes with indexes of dispersion," *Selected Areas in Communications, IEEE Journal on*, vol. 9, no. 2,pp. 203-211, 1991

[123] W. Li, R. J. Fretwell, and D. D. Kouvatsos, "Analysis of correlated traffic by batch renewal process," in *Proc. of International Conference on E-Business and Information System Security (EBISS)*, Wuhan, China, 2009, pp. 1-5. Available:http://ieeexplore.ieee.org/xpls/abs_all.jsp? arnumber=5137930&tag=1. [Accessed: 11 Apr. 2011].

[124] I. M. Mkwawa and D. D. Kouvatsos, "Broadcasting methods in MANETs: an overview," in *Network Performance Engineering - A Handbook on Convergent Multi-Service Networks and Next Generation Internet*, vol. 5233, D. D. Kouvatsos, Ed.: Springer, 2011, pp. 764-783.

[125] European Commission, "Challenge 2: cognitive systems and robotics, cooperation theme 3: ICT-information and communication technologies," Call from European Commission C(2010) 4900, 19 July 2010.

[126] J. Redi and J. Bers, "Exploiting the interactions between robotic autonomy and networks," in *Proc. of 2003 International Workshop on Multi-Robot Systems*, 2003, pp. 279-289. Available:http://www.ir.bbn.com/~redi/ papers/pdf/ RediBers_NRLMRS03 _ERNI.pdf. [Accessed :5 Jul. 2013].

[127] Y. Haiwen, Y. Haibin, and L. Xingshan, "Fuzzy Petri nets reasoning for application of electric control system fault diagnosis," in *Proc. of IEEE Conference on Robotics, Automation and Mechatronics*, Bangkok, 2006, pp. 1-6. Available: http://ieeexplore .ieee.org/xpls/abs_all.jsp? arnumber= 401 8795. [Accessed :14 Nov. 2012].

[128] Y. Ouchi and E. Tazaki, "Learning and reasoning method using fuzzy coloured Petri nets under uncertainty," in *Proc. of IEEE International Conference on Systems, Man*

and Cybernetics-Computational Cybernetics and Simulation, Orlando, FL,1997, vol. 4, pp. 3867-3871. Available: http://ieee xplore.ieee.org/stamp/stamp.jsp?tp=&arnumber =633274. [Accessed: 7 Dec. 2012].

[129] E. Cox, "Fuzzy fundamentals," *IEEE Spectrum*, vol. 29, no. 10, pp. 58-61, 1992.

[130] P. V. Subramanyam, A. Chauhan, and Y. Singh, "Modeling of a hybrid protocol for a using fuzzy Petri nets MANET," in *Proc. of Annual IEEE India Conference*, New Delhi, India, 2006, pp. 1-4. Available: http://ieeexplore .ieee.org/xpls/abs_all.jsp?arnumber=4086316. [Accessed: 15 Dec. 2012].

[131] J. B. Sinclair, 2004. Simulation of Computer Systems and Computer Networks: A Process-Oriented Approach. [Online eBook]. Available: http://www.google.co.uk/url?sa=t&rct=j&q=j.b. %20sinclair%202004%20simulation&source=web&cd=1&ved=0CC8QFjAA&url=http%3 A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.120.187 %26rep%3Drep1%26type%3Dpdf&ei=1aJUUeCKD9OS0QWojoGgDw&usg=AFQjCNG OfCHrzLQxOz8GkMweFHcLRtc4UA. [Accessed: 5 Feb. 2010].

[132] D. Dawoud, R. L. Gordon, and A. Suliman, "Trust establishment in mobile ad hoc networks: direct trust distribution-performance and simulation," in *Mobile Ad-Hoc Networks: Protocol Design*, X. Wang, Ed., 2011, pp. 513-564. Available: http://www.intechopen.com/books/mobile-ad-hoc-networks-prot ocol-design/trust-establishment-in-mobile-ad-hoc-networks-direct-trust-distribution-performance-and-simulation. [Accessed: 13 Apr. 2013].

[133] H. Lian and Z. Wan, "The computer simulation for queuing system," *World Academy of Science, Engeneering and Technology*, vol. 34, no. 1, pp. 176-179, 2007.

[134] R. Jain, *The Art of Computer Systems Performance Analysis*, vol. 182: John Wiley & Sons New York, 1991.

[135] K. Fall and K. Varadhan. NS-2 user manual. Available: http://www.isi.edu/nsnam/ ns/doc/ns_doc .pdf. [Accessed: 10 Oct. 2011].

[136] Omnet Community. Omnet++ user manual. Available: http://www.omnetpp.org /doc/omnetpp/ manual/ usman.html. [Accessed: 7 Nov. 2011].

[137] H. M. Deitel and P. J. Deite, *Java How to Program*, 7th ed. ed: Prentice-Hall, Inc., 2007.

[138] L. M. Leemis and S. K. Park, *Discrete-Event Simulation: A First Course*. Upper Saddle River, NJ: Pearson Prentice Hall, 2006.

[139] M. Zhou and K. Venkatesh, *Modeling, simulation, and control of flexible manufacturing systems: a Petri net approach*. Singapore: World Scientific Publishing Company Incorporated, 1999.

[140] Y. Narahari, K. Suryanarayanan, and N. V. S. Reddy, "Discrete event simulation of distributed systems using stochastic Petri nets," in *Proc. of the 4th IEEE International Conference on Energy, Electronics, Computers, Communications,* Bombay, India,1989, pp. 622-625. Available:http://ieeexplore.ieee.org/stamp/stamp .jsp?tp= &arnumber= 177017. [Accessed: 7 Nov. 2011].

[141] G. Chiola and A. Ferscha, "Exploiting timed Petri net properties for distributed simulation partitioning," in *Proc. of 26th Hawaii International Conference-System Sciences*, 1993, vol. 2, pp. 194-203. Available:http://ieeexplore. ieee.org/xpls/abs_all.jsp?arnumber=284110. [Accessed: 20 Jul. 2012].

[142] H. M. Cintra and V. W. Ruggiero, "A Tool for Modeling and Simulation of Computer Architectures Using Petri Nets," in *Proc. of the 7th Brazilian Symposium on Computer Architecture*, 1995. Available: http://www.lbd.dcc.ufmg.br/colecoes/sbac-pad/1995/0038.pdf. [Accessed: 20 Jul. 2012].

Appendix A Discrete Event Simulation Technique

A.1 Introduction

This appendix describes the simulation and validation of the models that have been used as basis for the rest of the simulation models throughout the thesis. Simulation is used in this thesis as an evaluation tool for the network performance and security trade-offs.

The simulation used in this study is a purpose-built DES written in Java. Generally speaking, simulation can be event-driven, process-oriented, or distributed [131]. DES was chosen since it is easy to construct and commonly used in the literature. DES Technique considers systems in which changes occur at discrete instances in time such as the arrival of messages at a router or a robotic node. This event, the arrival, will cause a change in the state of the router's model. During the time between these arrivals, the state remains unchanged [131].

Test beds/measurements are realistic tools for evaluating the performance and security of high-speed networks; however, it is impractical to configure them/set them up. In addition, when the size of the implemented nodes within the network is large, the evaluation process becomes expensive. Consequently, it is difficult to perform the comparison for various protocols under the same conditions. For these reasons, simulation is considered a better choice and is widely used for analysing complex networks [132].

Analytic models based on queueing theory provide elegant analytical solutions; nevertheless, as the system complexity increases, they may require a number of simplifying assumptions that must be made to derive equations for the performance metrics parameters. Simulation, on the other hand, is a more generic prediction tool which overcomes queueing theory's limitation and it can be used to model reality in greater detail [4]. This can be performed by constructing the system's model in the form of a program and calculating the measurements over time, and obtaining the performance metrics [132].

The simulation algorithms of GE random variable, QNs and SPNs are explained. In particular, the main building blocks for the models used throughout the thesis were validated against appropriate analytical solutions from the literature.

A.2 Features of Simulation

Generally speaking, the use of simulations can help reduce the development costs of a system as well as improve the safety of the experiments and debugging [133]. The main advantage of simulation is its ability to capture and track the dynamic behaviour of complex systems and evaluate them over time [134]. Several Simulation packages such as NS-2 [135], as its enhanced functionality is suitable for wireless scenarios", Omnet++ [136], GloMoSim [132] have been used in the literature on this subject and they provide an environment to design and compare proposed and existing protocols. Despite the large number of these simulation packages, the simulation used in this study is implemented using Java programming [137]; a purpose-built DES has been used for its flexibility and simplicity in programming besides its

ability to analyse complex systems. One of the limitations of the simulation is that the produced results mainly depend on the random generators used (c.f., [105]). Simulation programs have been constructed for simulating GE random variable besides QNs, G-QNs and SPNs models for the proposed models.

A.3 Simulation Models' Components

This section describes the simulation of the GE distribution besides the main building blocks used in the proposed models in this study. These models are GE/GE/c, Open QN with G-Queues, and SPNs. Validations of these models are also included.

A.3.1 Simulating GE-Type Distribution

The Algorithm $H_2 \rightarrow$GE(c.f., Appendix B), describes the steps for generating a GE-type random variable (RV) t by using an H_2–type distribution [20] with a large value of the tuning parameter k. GE validation is considered among the next simulation model of multiple servers.

A.3.2 Simulating GE/GE/c Queue

The simulation is based on the method proposed by Law and Kilton [105].

The structures of the simulation algorithms are presented in appendix C.

a) Validation of GE/GE/c/FCFS Queue with ME Solution [20]

The solution of a single class GE/GE/c/FCFS queue with c ($c \geq 2$) [20], provided in Appendix D, has been utilised to validate the simulation results with 95% CI. The validation results are shown in Figure A-1and the input parameters for GE/GE/c model are listed in Table A-1. The comparisons between the analytic solution presented in [20]and the simulation results are shown in Figure A-1. It is obvious that the simulation results match the analytic solution.

A-1 Table Input parameters for the GE/GE/C simulation program

Input parameters	
Mean arrival rate (λ)	[0.50 7 step 0.5]
SCV of arrival times	8
Mean service rate per server (μ)	8
SCV of service times	8
Number of Servers (c)	3

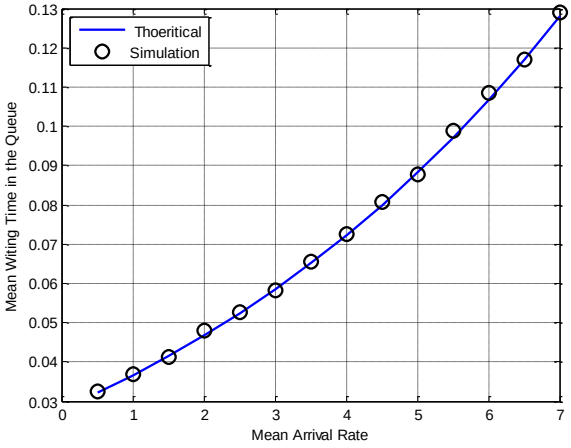


Figure A-1 The validation for the mean waiting time in the queue for GE/GE/c

A.3.3 Simulating Open Queueing Network M/G/1 FCFS with Single Class and G-Queues

In the context of this study, the simulation of open QN with G-queue, (c.f., Figure A-2), with multiple servers, SS and multiple classes and subject FCFS and HoL disciplines subject to arbitrary topology with infinite/finite capacity and RS-FD blocking mechanism where inter-arrival times and service times has GE distribution. This mode is based on the basic simulation algorithm for open QNs with single server and single queue with FCFS infinite capacity presented by Leemis [138].

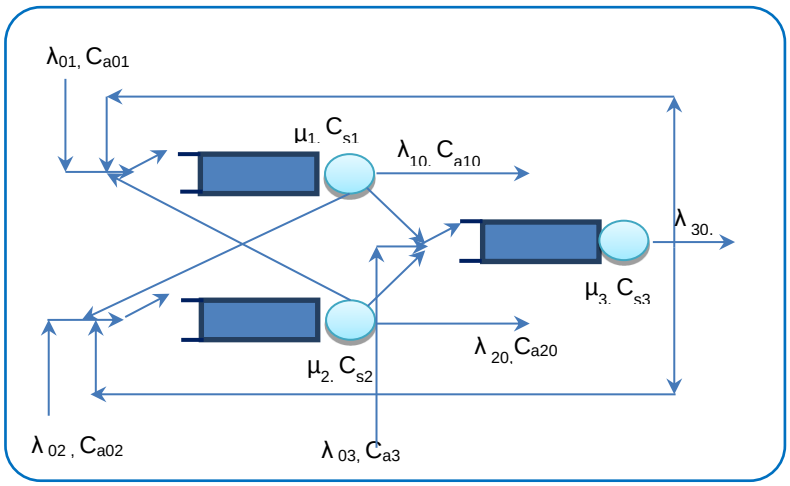


Figure A-2 The open QN model with multiple classes and gated queues

Security is modelled using delay centres and SS is also taken into consideration in the simulation program. Each service node has its own queue with infinite/finite capacity with its own type of queueing discipline (FCFS, HoL) and service time distribution. The simulation model construction is described in Appendix E.

a) Validation of the Simulated Model with GI/G/1/ FCFS Queue with Gates

An open QN model with k nodes each with single server and single class according to FCFS discipline has been validated against the analytic solution suggested by Bhatia (c. f.,[59]) as explained in Appendix F. Three G-QN nodes in mesh topology connected according to the topology are shown in Figure A-2, where the routing matrix, p, is specified by matrix p in Eq. A-1. The input parameters for the simulation programme are given in Table A-2. By validating the simulation results, with 95% CI, with the formulae provided by Bhatia, [18 , 59] and included in Appendix E, it can be seen they are nearly matched, as depicted in Figure A-3 and Figure A-4.

$$p = \begin{bmatrix} 0.0 & 0.33 & 0.34 & 0.33 \\ 0.236 & 0.0 & 0.412 & 0.352 \\ 0.23 & 0.308 & 00 & 0.462 \\ 0.274 & 0.4 & 0.326 & 0.0 \end{bmatrix} \qquad \text{Eq. A-1}$$

Table A-2 The input parameters for the Open QN model with gated-queues

Input parameters	
Mean arrival rate (λ) per node	From 1 to 4 with step 1
SCV of arrival times per node	3
Mean service rate per server (μ)	5
SCV of service times	1
Number of Servers (c)	1
Off rate (α) per node	0.1
On rate (β)	0.05
Number of nodes (N)	3

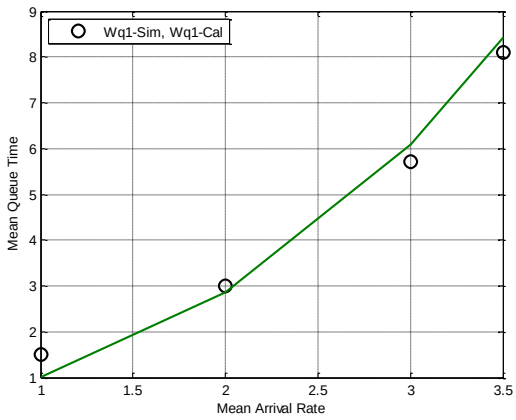


Figure A-3 The validation of mean queue time simulation for node 1

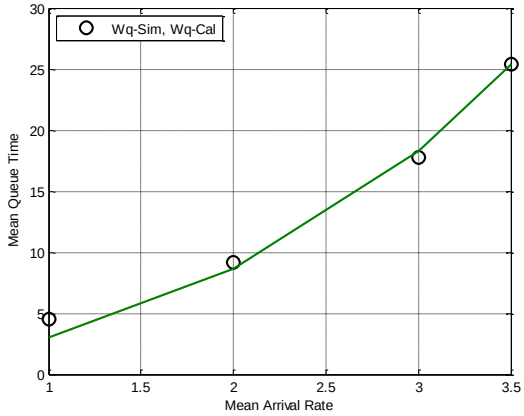


Figure A-4 The validation of the end-to-end queueing delay for the three nodes

A.3.4 Simulation of SPN

The simulation of SPNs (c.f., [139]), is structured as described in Appendix G. To simulate Timed Transitions PNs (TTPNs) in general and SPNs in particular, the correspondence between events and transition firing can be utilised [140], where events in DES occur when a transition fires.

a) Validation of SPN with GE/GE/1/N Solution

The GE/GE/1/N corresponding model is shown in Figure A-5Figure and the input parameters are listed in Table A-3.

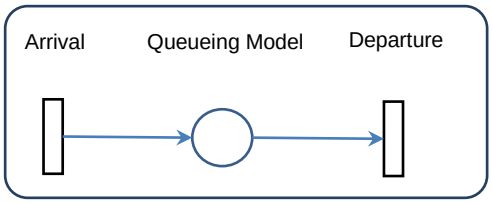


Figure A-5 The simulated SPN model

Table A-3 Input parameters for SPN validation

Input parameters	
Mean firing rate of t_1	[1-4 with step 1]
C_a^2	6
Mean firing rate of t_2	5
C_s^2	6
Place limit	50

The validation results for SPN (with general firing times - which are GE) against GE/GE/1/N ME solution [20] is depicted in Figure A-6.

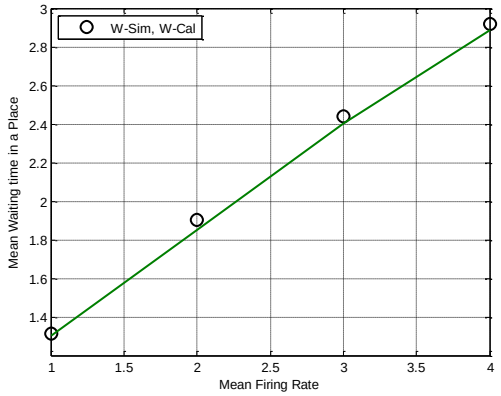


Figure A-6 The validation for the mean waiting time of tokens in a place

Appendix B GE Distributions

B.1 GE and H_2 Distributions

The PDF function of H_2 is given by[12]:

$$f(t,k) = \alpha_1(k)\upsilon_1(k)\exp\{-\upsilon_1(k)t\} + \alpha_2(k)\upsilon_2(k)\exp\{-\upsilon_2(k)t\}, t \geq 0 \qquad \text{Eq. B-1}$$

where 1/υ and C^2 are the mean and SCV and where k is a set of 'Tuning parameters' of H_2 family, k ∈ $(1,+\infty)$,α_1(k), α $_2$(k), υ_1(k) and υ_2(k) are given by Eq. E. B-4 to E. B-7 (c.f., [12]):

$$\alpha_1(k) = \frac{A+B}{C^2+1} \qquad \text{Eq. B-2}$$

$$\alpha_2(k) = 1 - \alpha_1(k) \qquad \text{Eq. B-3}$$

$$A = \frac{C^2-1}{2} + \frac{2}{k} \qquad \text{Eq. B-4}$$

$$B = \frac{1}{2}\left\{(C^2-1)^2 + \frac{8(C^2-1)}{k} + \frac{8(1-C^2)}{k^2}\right\}^{\frac{1}{2}} \qquad \text{Eq. B-5}$$

$$\upsilon_1(k) = k\alpha_1(k)\upsilon \qquad \text{Eq. B-6}$$

$$\upsilon_2(k) = \frac{k\alpha_1(k)\upsilon}{k-1} \qquad \text{Eq. B-7}$$

GE-type distribution can be considered an 'extremal' member of a family of two-phase H_2distributions with the same first two moments. When k→+ ∞, H_2→ GE [20]), i.e GE is an extremal case of an H_2 type distribution as shown in Fig. A.1.(c.f., by[12]).

$$\lim_{k\to+\infty(C^2>1)} f(t,k) \to \phi(t), \quad t \geq 0 \qquad \text{Eq. B-8}$$

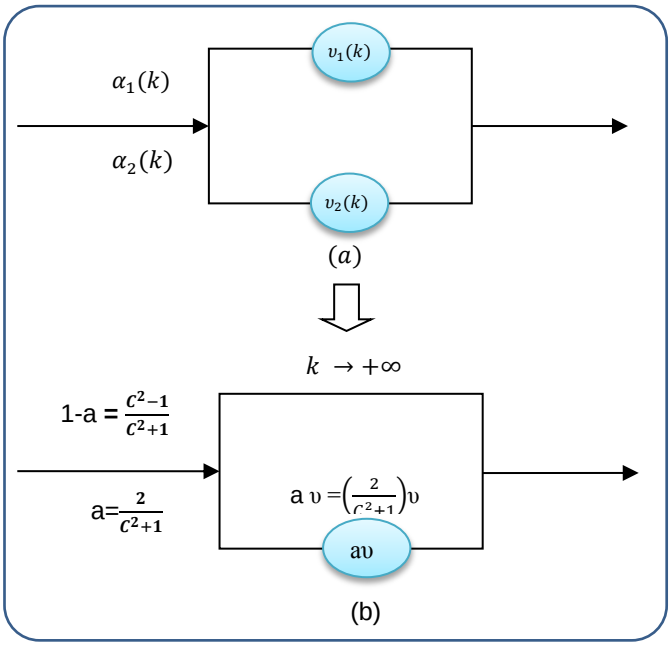


Figure B-1 The approximation of GE distribution using H_2 distribution with 'Tuning' parameter k ∈ $(1,+\infty)$(a) 2-phase Hyperexponential Distribution (b) GE-type distribution (c.f, [12])

B.2 The Relationship between IPP and GE

IPP can be fitted according to the inter-arrival time process into hyperexponential distribution [12 , 61 , 62]. Assuming X_i is the inter-arrival time between messages (i) and the message (i+1), the distribution of the inter-arrival time X_i is hyperexponential distribution (H_2) with cumulative distribution function[61 , 62]:

$$F(x) = \alpha_1\left(1 - e^{-\lambda_1 x}\right) + \alpha_2\left(1 - e^{-\lambda_2 x}\right), 0 < \alpha_1, \alpha_2 < 1 \qquad \text{Eq. B-9}$$

The four parameters of the hyperexponential distribution (λ_1, λ_2, α_1, α_2) are expressed in terms of IPP parameters (λ, α, β) as follows [61 , 62]:

$$\lambda_1 = \frac{\lambda + \beta_1 + \beta_2 - \delta}{2} \qquad \text{Eq. B -10}$$

$$\lambda_2 = \frac{\lambda + \beta_1 + \beta_2 + \delta}{2} \qquad \text{Eq. B -11}$$

$$\alpha_1 = \frac{\lambda^2 \beta_2}{\lambda\beta_2(\lambda_2 - \lambda_1)} - \frac{\lambda_2}{\lambda_1 - \lambda_2} \qquad \text{Eq. B -12}$$

$$\alpha_2 = 1 - \alpha_1 \qquad \text{Eq. B -13}$$

$$where \delta = \sqrt{\lambda + \beta_1 - \beta_2)^2 + 4\,\beta_1\beta_2} \qquad \text{Eq. B -14}$$

The mean E(t), variance Var(t), and C^2 of the hyperexponential distribution, in terms of IPP parameters, are[34]:

$$E(t) = \frac{\alpha_1}{\lambda_1} + \frac{\alpha_2}{\lambda_2} \qquad \text{Eq. B -15}$$

$$Var(t) = \frac{2\,\alpha_1}{\lambda_1} + \frac{2\,\alpha_2}{\lambda_2} - \left(\frac{\alpha_1}{\lambda_1}\right)^2 - \left(\frac{\alpha_2}{\lambda_2}\right)^2 \qquad \text{Eq. B -16}$$

$$C^2 = \frac{Var(t)}{E^2(t)} \qquad \text{Eq. B -17}$$

by equating the mean of GE (υ) to 1/E(t) of H_2 (i.e $\upsilon = 1/E(t)$), expressed by IPP parameters, from Eq. B-15 and calculating the C^2 for GE from Eq. B-17 (which gives the SCV of H_2 in terms of IPP parameters) and subtituting these values (υ and C^2) in Eq. B-2 to Eq. B-7 to obtain the corresponding values for $\alpha_1(k)$,$\alpha_2(k)$, A, B,$\upsilon_1(k)$, $\upsilon_2(k)$. In this way, GE r.v. is generated using H_2 r.v, whose parameters are expressed in terms of IPP, by making k → + ∞. i.e.:

IPP (λ, α, β) → H_2(λ_1, λ_2, α_1, α_2) → $H_2(\alpha_1(k), \alpha_2(k), \upsilon_1(k), \upsilon_2(k)) \rightarrow GE(When\ k \rightarrow +\infty)$

B.3 Generating a GE-type Distribution from a Family of H_2 Distributions with the Same First Two Moments

The Algorithm**H_2 →GE** is shown in Figure B-2, Figure B-3, with a large value of the k ≥ 1000 in order to generate proper GE RVs[12].

Begin

Step 1: Specify the values for υ and C^2 for the required GE-RV, X (c.f., Part 1);

Step 2: Input the value of the tuning parameter k;

Step 3: Calculate $\alpha_1(k)$, $\alpha_2(k)$, $\upsilon_1(k)$ and $\upsilon_2(k)$ using the specified values of υ and C^2 in Step 1;

Step 4: Generate $U_1[0,1]$ and $U_2[0,1]$ (uniformly distributed random variables);

Step 5: If $U_1[0,1] \leq \alpha_1(k)$, go to Step 6, otherwise to Step 7;

Step 6: Generate an exponential RV, X_1 with mean rate $\upsilon_1(k)$ using $U_2[0,1]$; go to End;

Step 7: Generate an exponential RV, X_2 with mean rate $\upsilon_2(k)$ using $U_2[0,1]$;

End

Figure. B-2 The simulation algorithm for GE RV[12]

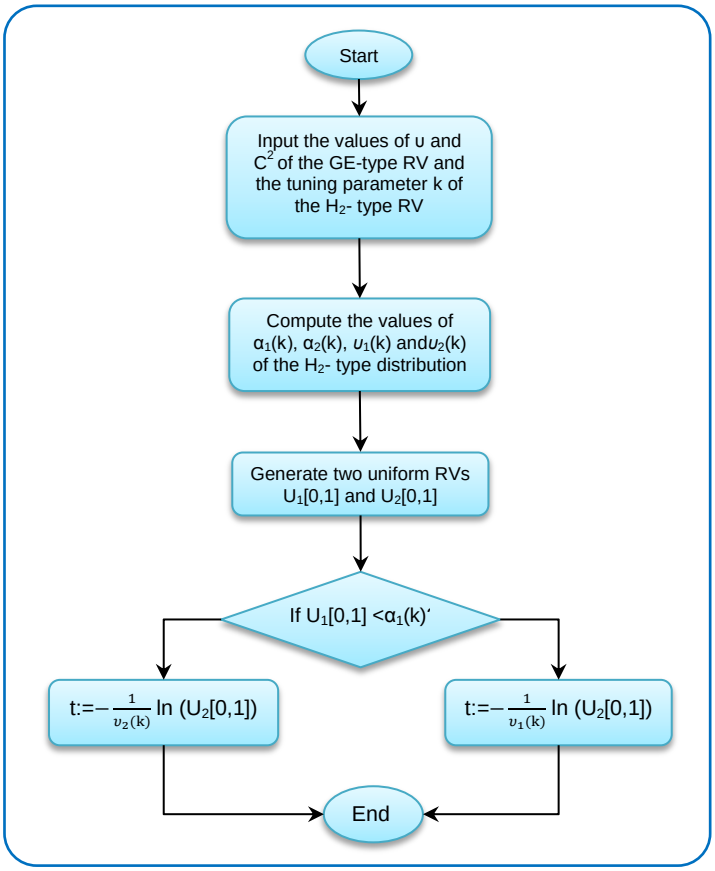


Figure B-3 The flowchart of algorithm $H_2 \rightarrow GE$ using H_2 distribution with 'tuning' parameter $k\ (1, +\infty)$ ([12 , 74 , 112])

Appendix C GE/GE/c Simulation Algorithm

The simulation algorithm for GE/GE/c is described below:

a) Main Function

The main function calls the timing function to determine the next event and then transfers control to the corresponding event function (which can be either arrival or departure) to update the system state appropriately. After simulation termination, report function is called to generate the results of interest [105].

```
Main Function()
BEGIN
   Initialise ()
/* Starting the loop */
WHILE  (num_customer<num_customer_required)  /*termination   condition*/
BEGIN
    Timing ()
If (next event type == 0)
   CALL Arrival()
 ELSE
CALL Departure()
     Update ()
     END WHILE
Report ()
END
```

Figure C-1 Main function structure for GE/GE/c simulation (adapted from [105])

b) Initialising function

This function initialises the simulation model at time zero.

```
Initialising function()
BEGIN /* initialize the state variables*/
  ENTER  Mean_ arrival = λ, Num_of_servers = c, SCVa=C_a^2;
  SCVs =C_s^2, mean_service rate for all servers
  num_customer_required,
  SET  sim_time=0.0, num_customer=0;
  num_in_q=0; server_status=0;  /*server status IDLE*/
  area_num in q=0 0; area_num_in_0.0; area_server_status=0.0;
  time_last_event=0.0; Q_Limit=1000; time_next_event[0]=sim_time +GE
   mean_interarrival, SCVa); /*Determine next arrival*/
For  I=1 TO c DO
     time_next_event[i]=max_double; /* Initialise  next departure*/
END FOR
END
```

Figure C-2 Structure of Initialising function of GE/GE/c simulation (adapted from [105])

c) Timing Function

It determines the next event is from the event list; the simulation clock is then advanced to the time of that event occurrence.

```
Timing function ()
BEGIN
int index; min= 1000000;
  FOR  I = 0 TO c DO
    BEGIN  (IF time_next_event [i]< min) THEN  next_event_type  = i;  /* the index of
the first idle server*/    END FOR
 Sim_time= time_next_event[next_event_type];
END
```

Figure C-3 Structure of Timing function of GE/GE/c simulation (adapted from [105])

d) Arrival Function

This function is called when arrival at the QN occurs, as shown in Figure C-4. Choose_Idle_Server function, shown in Figure C-5 is then called within this function to determine whether there is an idle server or not

```
Choose_Idle_Server function()
BEGIN
int index=0;
For  i=1 TO c DO
  BEGIN
    IF (ServerStatus(i) = False)   Index =i;  BREAK;
  END FOR
Return  index; /* record the index  of the idle server*/
 END
```

Figure C-4 Structure of Choose_Idle_Server function of GE/GE/c simulation (adapted from [105])

```
ArrivalFunction()
 BEGIN
num_customer ++;
Time_next_event[0] = sim_time+exp(lamda; K= ChooseServerIdle();
IF (k != 0)  /* If there is an idle Server
   BEGIN
    server_status [k]= 1; /* make server busy*/    time_next_event[k] = sim_time +
expon(mean_service[k]);  num_custs_delayed++;   END IF
ELSE IF ( num_in_q<Q_Limit)
 /* All servers are busy and the queue is not at full capacity*/
   BEGIN
   num_in_q ++;   time_arrival [num_in_q] = sim_time; END ELSE IF
END
```

Figure C-5 Structure of Arrival function of GE/GE/c simulation (adapted from [105])

e) Departure Function

This function, shown in Figure C-6, is called when a job departs from QN node.

```
Departure(Server)
BEGIN
IF (num in q == 0) /* queue empty*/
   BEGIN
     server_status [server]= 0/* server IDLE*/ time_next_event[server] = max_double;
   END IF
 ELSE /* serve a  job from the queue*/ num_in_q --;total_of_delays += (sim_time-
time_arrival[1]); num_custs_delayed ++;
     time next event[server] =sim_ time+expon(mean_service[server]);
  FOR  i=1 TO num_in_q DO time_arrival[i]=time_arrival[i+1];   END ELSE
END
```

Figure C-6 Structure of Departure function of GE/GE/c simulation (adapted from [105])

f) Update Function:

It calculates the server utilisation for GE/GE/c, as shown in Figure C-7.

```
Update()
BEGIN
   time_since_last_event = sim_time - time_last_event;
   time_last_event  =sim_time;  Busy_servers=0;
 FOR  server=1 TO c DO
     IF (server_status [server]==1) THEN
       Busy_servers++;  END FOR
     area_server_status += Busy_servers  *time_since_last_event;
END
```

Figure C-7 Structure of Update function of GE/GE/c simulation (adapted from [105])

g) Report Function:

It produces a report contacting the required performance metrics when the simulation ends, as shown in Figure C-8.

```
Report()
BEGIN
 U= area_server_status / (sim_time*c); /* Traffic Intensity*/
 average_delay_in_q = total_of_delays / num_custs_delayed ; /*Mean   Queueing Time*/
  average_number_in_queue = area_num_in_q / Sim_time; /* MQL*/
  server_utilization=area_server_status/sim_time; /* Server Utilisation*/
END
```

Figure C-8 Structure of Report function of GE/GE/c simulation (adapted from [105])

Appendix D ME Solution for GE/GE/c/FCFS Queue

For a single class GE/GE/c/FCFS queue with c (c≥ 2) homogeneous servers at equilibrium, let p(n) be the ME state probability, n ≥ 0, subject to normalisation, least number of busy servers probabilities, i.e. $u_j=\sum_{n=j}^{\infty} p(n)$, j = 1, 2, . . ., c, and mean waiting length, *Lq* constraints and it is given by"[20]:

$$p(n)=\begin{cases} 1+\left[\sum_{n=1}^{c-1} G_n+\frac{G_c}{1-x}\right]^{-1} & ,n=0 \\ p(0)\left[\prod_{j=1}^{c} g_j^{h_{j(n)}}\right]x^{Lq(n)}, n=1,2,\ldots. & \end{cases} \quad \text{Eq. D-1}$$

Where: hj(n) =1 if n ≥j, or 0 otherwise;

L_q(n)= n-c, if n ≥c, or 0 otherwise;

and $G_n=\prod_{j=1}^{n} g_j$, n=1,2,…..c and g_j, j=1,2,……c; and x are the Lagrangian coefficients corresponding to (u_j, j=1,2,3,….,c} and L_q are constraints.

The Lagrangian coefficients are determined by[20]:

$$g_i=\begin{cases} \frac{u_j-u_{j-1}}{u_{j-1}-u_j}=\frac{(\lambda_2+(j-1)\mu_2\beta_1)\alpha_2}{j\,\mu_2(1-\alpha_1\beta_1)}, j=1,2,\ldots..c-1, \\ \frac{u_c(1-x)}{u_{c-1}-u_c}=\frac{(\lambda_2+(c-1)\mu_2\beta_1)\alpha_2}{\lambda_2\alpha_1+c\,\mu_2}, j=c, \end{cases} \quad \text{Eq. D-2}$$

$$x=\frac{\lambda_2+c\beta_1\mu_2}{\lambda_2\alpha_1+c\,\mu_2} \quad \text{Eq. D-3}$$

Eq. D-4

Where: u_0=1, $\mu_2=\alpha_2\mu$, $\alpha_2=2/(cs+1)$

$$\alpha_1=1-\alpha_2,\ \beta_2=\frac{2}{ca+1},\ \beta_1=1-\beta_2 \quad \text{Eq. D-5}$$

Appendix E Simulation Algorithm for Open Queueing Network GE/GE/1 FCFS with Single Class and Gated Queues

E.1 Simulation Description

The single-server service nodes are indexed s = 1, 2... k. Index s=0 is reserved for 'Super node' for external arrival and departure. The set of service nodes is denoted S = [1, 2,…., k] with S_0 = S = 0,1, 2,…, k. The service rate of node s ∈ S is μ_s. There is a (k + 1)× (k + 1) node transition matrix p defined in such a way that each job leaving node $s \in S_0$ will transition to node $\acute{s} \in S_0$ with probability [138]:

$$p[s,\acute{s}] = \Pr(transition\ from\ node\ s\ to\ node\ \acute{s}) \qquad \text{Eq. 8E-1}$$

By convention p[0, 0] = 0.

This matrix represents the network topology, as shown in Eq. C.2, and each row of p must sum to 1.0.

$$\text{p=}\begin{bmatrix} 0 & p[0,1] & p[0,2] & p[0,3] & \dots & p[0,k] \\ p[1,0] & p[1,1] & p[1,2] & p[1,3] & \dots & p[1,k] \\ p[2,0] & p[2,1] & p[2,2] & p[2,3] & \dots & p[2,k] \\ . & . & . & . & \dots & . \\ p[k,0] & p[k,1] & p[k,2] & p[k,3] & \dots & p[k,k] \end{bmatrix} \qquad \text{Eq. E-2}$$

p matrix should be converted to a cumulative node transition matrix P, as in **Algorithm I** (c.f., Figure E-1). This cumulative node transition matrix can then be used to simulate the node-to-node transitions of jobs as they move into, though, and out of the network, as in **Algorithm II** (c.f., Figure E-2).

Algorithm I:

```
P_construction_function()
BEGIN
FOR x=0  TO K DO  / *looping over rows*/
  BEGIN
  P[x,0]=p[x,0]; / * elements of the 1st column are identical to     those in p
    matrix
        FOR y=1 TO k  DO  / * looping over columns */
            P[x,y]=P[x,y-1]+p[x,y];  /* convert from  Probability Density Function
(PDF)to Cumulative Distribution Function (CDF)*/
        END FOR
      P[x,k]=1.0; /* last column elements*/
   END FOR
END
```

Figure E-1 the algorithm of selecting the next node in simulating an OQ network with random topology (adopted from [20])

Algorithm II:

```
Next_Node function()
 BEGIN
   U= Random();
   Y=0;
   WHILE (P[x,y] <u) DO
     BEGIN WHILE
       Y++ ;
    END WHILE
   Return y;
END
```

Figure E-2 The selection algorithm of the next node (adopted from [20])

It is worth pointing out that the number of network service nodes can be arbitrarily large; the network topology can be arbitrarily complex. Each node has a gate, which is either 'On' with rate β or 'Off' with rate α. Next-event simulation of a network of single-server service nodes with Gated Queue (G- queues)[18 , 59]can be constructed under the following assumptions: The simulation model of QN with G-Queues is described in Figure D-3, where the main function calls the sub-functions: Initialisation, timing, arrival, departure, transition, update, and report.

D.2 Simulation Algorithm

The simulation algorithm of OQN with gated queue is described in detail below:

- **Main Function**

The main simulation algorithm of QN Model with G-queue is shown in FigureE-3.The main difference between this program and the GE/GE/C program is as follows: In arrival() function, there is a need to call Find_Next_Node (0) function passing the first row of the routing matrix, while in departure(s) function Find_Next_Node (s) is called with passing 's' row number. G-Queue [59 , 88], can be simulated in a similar way to M/M/1 [105]. The main difference is that the arrival of jobs will be interrupted. The functions of Initialise, Timing and Arrival need to be modified to reflect the interruption event within them. Moreover, a new function called Transition is added. An outline of the simulation algorithm is presented below.

```
Main()
BEGIN
Initialization();
WHILE (Arrivals < Arrivals_Required)
    BEGIN WHILE
  timing();  /* determine the type of next event*/
  S= next_event_type() ;
     IF (S== 0) THEN
       CALL arrival();  /*external arrival to node s'*/
   ELSE IF (S>= 1) AND(S<=N) THEN  CALL departure(S);/* departure from s*/
     ELSE CALL transition();
    END  WHILE
  report();
 END
```

Figure E-3 The main function of simulating Open QN model (adopted from [138])

- **Initlisation Function**

This function initialises the nodes as well as defining the topology through p matrix and the two-dimension event list. In addition, it then schedules the arrival at each node and assumes all servers are idle. It also indicates the number of servers per node and the discipline per node (either HoL or FCFS). Finally, the gates for all nodes are assumed to be 'On'.The concept of the two-dimension event list was used, and the structure for this list is depicted in Figure E-4.

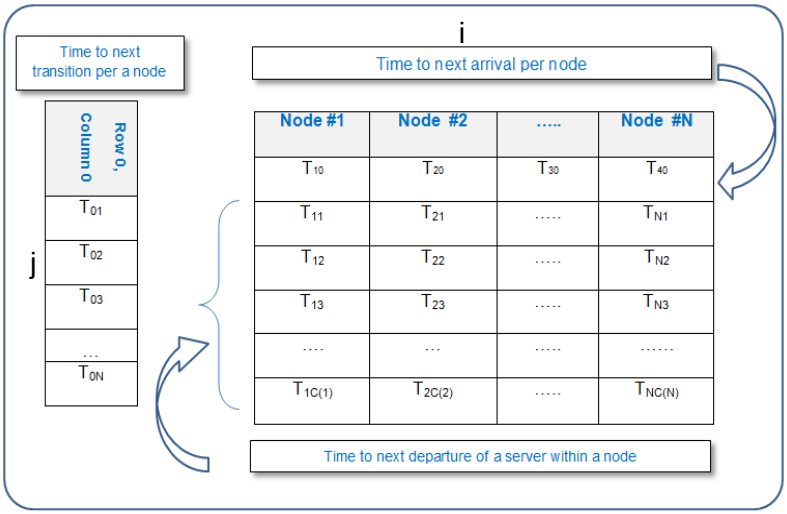


Figure E-4 The event list for simulating an Open QN model with arbitrary topology and G- queues

If column j = 0 and row i > 1, it means the next event is an external arrival at node # j.If column number j > 0 and row number i > 0, this indicates a departure from the server # j of node # i.If column number j = 0 and row number i >1, this mean the gate of a node j will be either 'Off' if it is already 'On' or vice versa.

- **Timing Function**

This function searches through the whole event list to determine the time and type for the next event, which is the minimum time among all values; it then records its row and column indexes/ numbers. According to the row and column indexes, either arrival, departure or transition functions will be called.

- **Arrival Function**

This function is called when arrival at the QN occurs, after which the system state is updated accordingly. The arrival of a new job is then scheduled according to GE distribution. If the nodes' gate is 'Off', the job is discarded; otherwise, it is served if the server is idle or queued otherwise.

- **Departure Function**

In this case, the server that performed departure from a particular node is made idle if there are no jobs in the queue; otherwise, another job is selected from the queue according to the service discipline, and its departure time is then scheduled. The job departing from the current node is routed to another node according to the routing matrix (i.e. the arrival function is performed to deal with the departed job). If the current node is not connected to other nodes, the departed job will not be traced /considered any further.

- **Update Function**

It calculates the server utilisation besides the overall utilisation in a similar way to GE/GE/c queue simulation.

- **Report Function**

Performance metrics that can be obtained are Lq, Wq, U, in a similar way to single node GE/GE/c, but they are calculated for each single node.

- **Transition Function**

. If the column number (j) = 0 and the row is between 1 and N, this means the gate of a node j will be either 'Off' if it is already 'On' or vice versa, as shown in Figure E-5

```
Transition Function()
BEGIN
    IF (state ==1) THEN   /* On State*/  state =2;/* Off State*/
       ELSE    state=1;   END IF
         time_next_event[3]=sim_time+expon(rate[state]); /* Schedule the next
transition for the corresponding state*/
END
```

Figure E-5 The simulation algorithm for the transition function

Appendix F The Solution of Open QNs with Gates

The effective mean arrival rate and SCV for a node with gate is calculated as follow[59]:

$$\lambda_j = \lambda_{0j} + \sum_{i=1}^{M} p_{ij}\acute{\lambda_i} \quad \text{Eq. F-1}$$

$$C_{aj}^2 = a_j + \sum_{i=1}^{M} b_{ij}C_{ai}^2 + k\sum_{i=1}^{M} b_{ij}\,\lambda_i \quad \text{Eq. F-2}$$

Let $\acute{\lambda}_j$ denotes the mean arrival rate of the interrupted arrival process, due to the On-Off gate and $C_{aj}^{\acute{2}}$ is the effective SCV of the arrival process at node j.The total arrival rate λ_j at node j due to external and internal traffic flows at node j is given by[59]:

Where $$\acute{\lambda_J} = p_{on}\,\lambda_j \quad \text{Eq. F-3}$$

and $$p_{on} = \frac{\beta}{\alpha+\beta} \quad \text{Eq. F-4}$$

The utilisation per node is calculated as:

$$\rho_j = \frac{\acute{\lambda_J}}{\mu_j} \quad \text{Eq. F-5}$$

Where: $$k = \frac{\alpha\,(\nu_{on}\,\alpha^{\,2} + \nu_{off}\,\beta^2)}{(\alpha+\beta)^2} \quad \text{Eq. F-6}$$

Where a_j and b_{ij} are derived after considering merging and splitting of traffic streams and are given as follows[59]:

$$a_j = 1 + \omega_j\left\{\left(q_{0j}C_{0j}^2 - 1\right) + \sum_{i=1}^{M} q_{ij}\left[\left(1-p_{ij}\right) + \left(p_{ij}\rho_i^2 x_i\right)\right]\right\} \quad \text{Eq. F-7}$$

$$b_{ij} = \omega_j p_{ij} q_{ij}(1-\rho_i^2) \quad \text{Eq. F-8}$$

$$x_i = max_{1\le i\le M}(C_{si}^2, 0.2) \quad \text{Eq. F-9}$$

$$\omega_j = \left[1 + 4(1-\rho_i)^2\left(\nu_j - 1\right)\right]^{-1} \quad \text{Eq. F-10}$$

$$\nu_j = \left[\sum_{i=0}^{M} q_{ij}\right]^{-1} \quad \text{Eq. F-11}$$

Thus it is possible to calculate the mean waiting time at node j by[59]:

$$W_{qj} = \frac{\lambda_j\left(C_{aj}^2 + C_{sj}^2\right)g_j}{2\left(1-\rho_j\right)} \quad \text{Eq. F-12}$$

The mean waiting time of a customer in a network, W_s, (i.e., the End-to-End Delay) is given by:

$$W_s = \sum_{j=1}^{M} W_{sj}, \quad \text{Eq. F-13}$$

Where the mean response time per node, W_{sj}, is given by[59]::

$$W_{sj} = W_{qj} + \frac{1}{\mu_j} \quad \text{Eq. F-14}$$

Appendix G Simulating SPNs

F.1 Simulation Description

Similar to the QN simulation concept, simulating SPN require the creation of an event list and scheduling the transition firing and executing the firing event for the transition with minimum firing time. According to the fired transition, the network marking is updated and the list of newly enabled transitions is updated (enabled transitions may become disabled and vice versa). Consequently, new events are inserted into the event list and old events are removed from the list. The simulation time (or clock) is advanced to the next event timestamp. This is given by the sum of the current simulation time and the minimum remaining firing time of the enabled transition[141]. It is worth mentioning that the topology of SPN is defined through input and output functions, which specify the connectivity between places and transitions, as described below[139 , 142]:

$$I(t,p) = \begin{cases} 1, there\ is\ an\ arc\ connection\ for\ (t,p) pair \\ 0, there\ is\ no\ arc\ connection\ for\ (t,p) pair \end{cases} \quad \text{Eq. G-1}$$

A simple example depicted in Figure G-1 shows how to define I(t,p) and O(t,p), which are expressed in Eq. G-2:

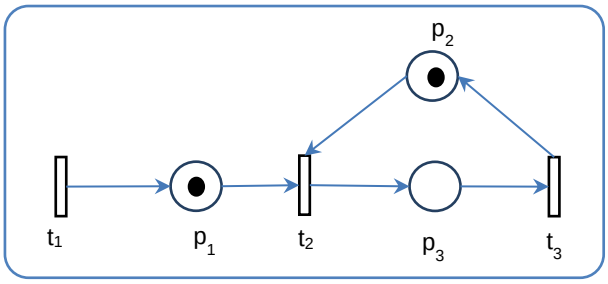


Figure F.1 An example on defining SPN topology (adopted from [139]

$$I(t,p) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, O(t,p) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{Eq. G-2}$$

F.2 Simulation Algorithm

- **Main Function**:

It coordinates the functioning between sub-functions and generates a report of the system elements and the corresponding performance metrics, shown in Figure-G2[139 , 142]:.

```
Main()
BEGIN
Initialisation(); /* Setting imitating SPN /*
WHILE (Termination Condition is not met)  DO
  BEGIN
     Check_newly_enabled_transitions() /* Check for newly enabled     transitions and
     generate  the firing time them */
```

```
     Timing(); /* determine the transition with the minimum remaining firing time */
     Firing() /*  perform the firing for the selected transition
      Update()/*update SPN according to the new marking
   END WHILE
Report(); /*Calculate  performance metrics*/
END
```

Figure G-2 simulation algorithm of SPN (adapted from [139])

- **Initlisation Function**

This function initialises the marking of the SPN and defines the topology through Input and Output matrixes. It also then checks for the transitions, which are enabled by default (which do not have input places), and enables them throughout the simulation, as well as generating the firing times for them. Firing rates for transitions are initialised. Figure G-3 outlines the tasks of this function.

```
Initialise function ()
Step 1: initialise  Global and local clock to zero and set initial marking;
Step 2: initialisation all counters and variables used to determine required metrics;
Step 3: define the SPN topology through I(t,p), O(t,p) functions;
Step 4: Return to the main function.
```

Figure G-3 The simulation algorithm for initialise function(adapted from [139])

- **Check Newly Enabled Function**

The main task of this function is to check for newly enabled transitions after updating the marking of SPN, i.e. by checking the enabling function in which all input places for each transition are checked to determine whether they contain the required number of tokens. Once found, exponentially distributed firing times are generated to these enabled transitions according to their firing rates. Consequently, a list of enabled transitions is created and their firing times are recorded in local timers, as shown in Figure G-4.

```
check_newly_enabled_transitions function ()
Step 1: searching for the transitions that are enabled by default    (i.e. without
input places) and putting them in a special array
(enabled_transitions_by_default);
Step 2: Check for previously enabled transitions whether they become disabled for the
current marking;
Step 3:  generate firing times for these transitions;
Step 4: for those transitions have input places check  for each transition whether
its input places have at least one token;
Step 5: the enabled transition are listed in an array (newly_enabled_transitions)and
the firing time for them are generated;
Step 6: Return to the main function.
```

Figure G-4 The simulation algorithm for Check_newly_enabled_transitions function(adapted from [139])

- **Timing Function**

This function, presented in Figure G-5, searches through the whole SPN network for the transition with the minimum remaining firing time and then records its index.

```
Timing function()

Step 1: Loop for all newly enabled transitions;
Step 2: find the transition with the minimum firing time;
Step 3: record the transition index and the firing time;
Step 4: Return to the main function.
```

Figure G-5 The simulation algorithm for Timing function (adapted from [139])

- **Firing Function**

The firing process is performed in this function, as depicted in Figure6-G.

```
Firing function()
Step 1: Update the Global clock to be synchronised with the firing time for the selected transition in ( Timing Function);
Step 2: decrease the minimum firing time from local times for all enabled transitions;
Step 3: if the fired transition is enabled by default, generate a new firing time for it, otherwise make it disabled;
Step 4: Update the counters to calculate the performance metrics at the current simulation time;
Step 5: Update the marking of SPN (by decreasing one token from each input place for the fired transition and increasing the number of tokens for its output places;
Step 6: Return to the main function.
```

Figure G-6 The simulation algorithm for Firing function (adapted from [139])

- **Update Function**

The simulation time will be updated by adding the minimum firing time in the previous function. All firing times of the transitions will be reduced by the amount of the minimum firing time. These tasks are outlined in Figure G-7.

```
Update function()
Step 1: Update the local clocks (times) for each enabled transition by decreasing the minimum firing time from their firing times;
Step 2: Update the statistics, as shown below in the performance calculations;
Step 3: Return to the main function.
```

Figure G-7 The simulation algorithm for Update function (adapted from [139])

- **Report Function**

The statistics will be updated in the way shown in Figure G-8.

```
Report function()
Step 1: Calculate the mean number of tokens in a particular place by  Eq. A.1;
Step 2: Calculate the mean waiting time in a place by Eq.A.2;
Step  3:  Calculate  the  fraction  of  time  that  a  transition  is  enabled  by  Eq.A.3;
Step 4: Calculate the throughput of a given transition  Eq.A.4
Step 5: Return to the main function.
```

Figure G-8 The simulation algorithm for Report function (adapted from [139])

The obtained performance metrics from the simulation are [142]:

1- Mean number of tokens in the place: This corresponds to the mean response time in QNs and it is expressed by mean number of jobs/ simulation time, i.e.[142]:

$$N_M = \frac{\sum M * \tau}{T_s} \qquad \text{Eq. G-1}$$

2- Mean waiting time in the place

This is calculated by: mean number of jobs in the place divided by the number of tokens in that place[142]::

$$T_J = \frac{\sum M * \tau}{N_\tau} \qquad \text{Eq. G-2}$$

where M is the number of tokens at the beginning of the cycle, τ is the duration of the cycle, and N_τ is the number of different tokens that have passed through this place until the current cycle. So, calculating the sum ($M * \tau$) at each cycle at the end of the simulation. The value of Nt can be obtained by incrementing a counter each time an input transition fires and puts tokens in the place.

3- Transition utilisation: This is the fraction of time during which a transition is enabled, and it is expressed by duration of firing time for a transition / simulation time, i.e.[142]:

$$U_j = \frac{\sum F_j}{T_s} \qquad \text{Eq. G-3}$$

Where F_j is the firing time for a transition j

4- Transition throughput: This metric can be defined as the 'number of firing times divided by the simulation time', i.e., [142]:

$$T_F = \frac{N_F}{T_s} \qquad \text{Eq. G-4}$$

Where T_S is the simulation time and N_F is the number of firings of the transition.