Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 4582391, 14 pages
https://doi.org/10.1155/2019/4582391

Research Article

Policy-Based Security Management System for 5G Heterogeneous Networks

Hani Alquhayz,[1] **Nasser Alalwan**,[2] **Ahmed Ibrahim Alzahrani**,[2] **Ali H. Al-Bayatti**,[3] **and Mhd Saeed Sharif**[4]

[1]*Department of Computer Science and Information, College of Science in Zulfi, Majmaah University, Al-Majmaah 11952, Saudi Arabia*
[2]*Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia*
[3]*School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK*
[4]*School of Architecture, Computing and Engineering, UEL, University Way, Dockland Campus, London E16 2RD, UK*

Correspondence should be addressed to Ahmed Ibrahim Alzahrani; ahmed@ksu.edu.sa and Ali H. Al-Bayatti; aalbay00@gmail.com

Received 13 August 2019; Accepted 23 October 2019; Published 14 November 2019

Guest Editor: Hasan Ali Khattak

Advances in mobile phone technology and the growth of associated networks have been phenomenal over the last decade. Therefore, they have been the focus of much academic research, driven by commercial and end-user demands for increasingly faster technology. The most recent generation of mobile network technology is the fifth generation (5G). 5G networks are expected to launch across the world by 2020 and to work with existing 3G and 4G technologies to provide extreme speed despite being limited to wireless technologies. An alternative network, Y-Communication (Y-Comm), proposes to integrate the current wired and wireless networks, attempting to achieve the main service requirements of 5G by converging the existing networks and providing an improved service anywhere at any time. Quality of service (QoS), vertical handover, and security are some of the technical concerns resulting from this heterogeneity. In addition, it is believed that the Y-Comm convergence will have a greater influence on security than was the case with the previous long-term evolution (LTE) 4G networks and with future 5G networks. The purpose of this research is to satisfy the security recommendations for 5G mobile networks. This research provides a policy-based security management system, ensuring that end-user devices cannot be used as weapons or tools of attack, for example, IP spoofing and man-in-the-middle (MITM) attacks. The results are promising, with a low disconnection rate of less than 4% and 7%. This shows the system to be robust and reliable.

1. Introduction

5G is the fifth-generation cellular network technology, and the International Telecommunication Union (ITU) has designated the International Mobile Telecommunications-Advanced (IMT-Advanced) standard as the global standard for 5G wireless communications. The ITU Radiocommunication Sector (ITU-R) has specified that 5G must [1]

(i) Provide features such as high mobility
(ii) Be ultrareliable and have ultralow latency (1 ms)
(iii) Have a high peak data rate of 10–20 GB

Many 5G providers are attempting to build systems that satisfy these requirements, particularly high speed, but these lack convergence between wireless and wired networks. However, Y-Communication (Y-Comm) architecture, developed at Cambridge University, allows for heterogeneous networking. It consists of a fast core network and a slower peripheral network [2].

Our system includes optical networks and peripheral networks and uses wireless technologies such as 5G [3], which is the main component of the core network. The current security weaknesses in 4G have been investigated thoroughly in [4–6]. However, to date, there are no real

security provisions for 5G heterogeneous mobile networks. Y-Comm includes a security solution that uses a multilayer security system, but research has demonstrated that several security threats could result in service interruption and the expropriation of data.

The research has further demonstrated that current and new perceived threats to security are intrinsic to 5G technology [7]. ETH Zurich, the University of Lorraine/INRIA, and the University of Dundee found that criminals will be able to intercept 5G communications and steal data due to multiple security gaps. According to a press release issued by the group, this is in part because "security goals are underspecified" and there is a "lack of precision" [8]. Therefore, the security specifications of 5G heterogeneous networks can be classified into two levels; the first is associated with mobile equipment and the second with operator networks. Moreover, a number of mobile equipment security specifications need to be considered, such as guaranteeing a device's integrity, privacy, and confidentiality; ensuring controlled access to data; and preventing the mobile equipment from being stolen or compromised, and the data from then being compromised or used as a tool for aggression. Authentication and authorisation on the interface between the network and the operator have been the main focus of security research carried out on 5G heterogeneous networks.

There is a critical commercial need to create a comprehensive security management system for 5G heterogeneous networks, and we have therefore developed

(i) A policy-based security management system that identifies whether a mobile device has been used as an attacking tool in the Y-Comm environment. This follows ITU-T recommendation M.3400 to deal with security violations in the network.

(ii) A novel intelligent agent (IA) mechanism to detect malicious behaviour in an end-user device.

(iii) A self-managed cell for the Y-Comm network to interact with managed objects. The self-managed cell is represented as a policy feedback loop, which is triggered by the end-user device.

The rest of this paper is structured as follows. Section 2 contains background information about the security problems related to 5G heterogeneous networks, ITU-T recommendations, and policy-based systems. Section 3 presents the critical analysis of related work. Section 4 clarifies the Y-Comm framework. In Section 5, we illustrate the results, and in Section 6, we show the testing performance. Our conclusions will also be presented in Section 7.

2. Background

The following section will discuss all related aspects of this paper, starting with 5G networks and ending with Ponder2 (the second version of Ponder).

2.1. 5G Networks. Information and communication applied sciences have sparked innovations worldwide. The ever-growing ability to instantly transfer and process facts is transforming society in many ways, including online shopping, social interactions, media distribution, e-learning and m-learning, and audio and video communication. Industry and business have been based primarily on technological advancements. In attempting to satisfy increasing user requirements, it is becoming extremely difficult to ignore what is required in next-generation wireless communications [9].

Next-generation 5G wireless communications face a challenge in achieving very high data rates, low latency, an increase in base station capacity, and improved QoS in comparison to current 4G in attempting to satisfy increasing user requirement (LTE) networks.

Major industries, researchers, and vendors have determined the key requirements of the next-generation 5G systems, which are as follows:

(i) Up to 10 Gbps data rates in realistic networks (10a 10-fold increase compared with an LTE network) [7]

(ii) High bandwidth in unit areas compared with 4G [10]

(iii) A massive number of subscribers to connected devices in order to realise the imaginative and prescient Internet of things (IoT) [11]

(iv) 1 ms round trip latency—roughly 10 times less than LTE's 10 ms round trip time;

(v) Wide coverage ("anytime anywhere" connectivity)—5G wireless networks should provide almost 100% coverage

(vi) Reduction in power consumption by almost 90%

With the abovementioned requirements, wireless industries, as well as academia and research companies, have started cooperating regarding the one-of-a-kind aspects of the 5G wireless structure. In 5G, virtually all communication spectrums can be used more efficiently and can be categorised as vertical and horizontal sharing. Vertical sharing refers to spectrum sharing between users of different priority (e.g., primary and secondary), that is, unequal rights of spectrum access. Horizontal sharing is sharing between systems that have the same priorities; namely, different users have equal access rights. If the users in the spectrum adopt the same technology, it is called homogenous horizontal sharing; otherwise, it is called heterogeneous horizontal sharing [12].

2.2. Y-Comm Architecture. A group of researchers from the Networking Research Group at Middlesex University, the Computer Laboratory at Cambridge University, Samsung Research and Deutsche Telekom, introduced the Y-Comm framework. The objective of this framework is to address new challenges in heterogeneous networks. There are challenges in many areas, including the network, device, and application levels. The framework maintains a layered approach and performs as a reference model, as in the Open Systems Interconnection (OSI) reference model [13]. In this study, we propose a security management system for the Y-Comm framework.

Given that different operators will own the future heterogeneous networks, new network operators will be able to join the core network. However, this raises the issue of interoperability between these different operators. ITU-T addresses this issue, recommending a central management entity that works as a regulatory authority with the power to enforce policies in the network and implement service and network-level agreements to control the entire network. Y-Comm follows this concept by proposing a core endpoint to work as an administrative entity to control the peripheral networks [14]. Our proposed policy-based system enforces policies in the Y-Comm architecture using this administrative entity.

Figure 1 shows the structure of the Y-Comm network, which contains the core endpoint at the top and the peripheral networks at the bottom. The peripheral networks provide the service to the end users via access routers (ARs). The middle level contains domains, with each one representing a network operator. The most important components in this research are the central A3C server (CA3C) and the AR. Other components address other issues in the network, such as QoS and handover. The CA3C server is the central authentication, authorisation, accounting, and cost system; it also contains the service-level agreements (SLAs) and network-level agreements (NLAs). SLAs specify the terms on which the clients use the service, and NLAs specify the terms on which the clients access the networks [14]. The AR is the link between the network provider and the end-user device, and it is responsible for enforcing admission control decisions. Additionally, the AR acts as the authenticator for network users after receiving permission from the CA3C server in the core endpoint.

2.3. Analysis of Y-Comm and 5G Networks. Owing to its open nature, the 5G infrastructure can be accessed from a range of external connection points through peer operators, the Internet, and third-party technologies. All these represent security vulnerabilities in the system, and, because service providers use the same core network infrastructure, if a single provider is under threat, this would affect the whole network infrastructure [4]. To overcome such threats, the Y-Comm research group has developed a security system, although the solutions are not comprehensive. Aiash et al. focused their research on the security difficulties found in 4G systems. Their approach to resolving these difficulties involved applying existing security techniques to 4G networks, as they discovered that existing and new security threats were intrinsic only to 4G technology. They examined the idea of applying the authentication and key agreement (AKA) of 3G to a 4G communication framework using standard X.805. By doing this, they were able to analyse the AKA protocol in 4G networks. They consequently discovered a significant number of threats to the network's security [5]. Moreover, Park et al. discovered that because 5G is an IP-based and heterogeneous network, a variety of security threats exist that have the potential to interrupt service and allow data to be expropriated. In addition, they investigated and suggested solutions for a number of ongoing open problems that need to be solved [4].

In a traditional network, security is achieved by not allowing threats to access network entities. However, in a 5G open-architecture network, this is ineffectual because the attackers attempt to discover security vulnerabilities in the operating system, network protocols, and applications, and by exploiting them, they can develop malware that attacks and abuses the network. The new architecture identifies possible threats within a 5G network system, including IP address spoofing, user ID theft, theft of service (ToS), denial of service (DoS), and intrusion attacks. Due to the open architecture and IP-based environment, 5G heterogeneous networks are subject to new security threats and inherit existing threats from the Internet. Given that the network infrastructure was the property of the service providers and access to other network equipment was prohibited, these threats were never present in 3G and 4G networks. In addition, there is an increase in security threats because of the diversity of end-user devices and security levels [15]. Experience relating to Internet protection indicates that protection needs to incorporate data and entities, which suggests that the 5G network should preserve both the entities and infrastructure [4].

An additional security problem arises in mobile communications when an end-user device is disconnected from the network for any reason, for example, if the device has run out of battery. Moving from disconnected to connected status on a mobile device provides an opportunity for an attacker to simulate a mobile device or a mobile support station [3]. The emergence of root kits, malware capable of modifying operating system codes and data for malicious reasons, has made it even more important to protect end-user devices. According to McAfee, the use of root kits has increased by 600% over the last few years [16] and the majority of malware seems to target Android operating systems [17]. Furthermore, new end-user devices are becoming sources of DoS attacks, viruses, and worms, with smart phones becoming attractive targets. As a result, there is an increasing number of harmful social implications that must be addressed. Y-Comm and Hockey have proposed some security solutions for heterogeneous mobile networks. However, these solutions do not consider the security of end-user devices, which are the source of numerous security weaknesses, and do not meet the security standards of 5G systems.

2.4. Policy Overview. This paper details a policy-based system to cover the vulnerabilities in security systems for heterogeneous networks. The convergence between wired and wireless technologies in 5G heterogeneous networks and the diversity of network technologies make managing these networks complex. The intricacies involved have encouraged researchers to find an appropriate network management technique. Policy-based management systems have become promising solutions for controlling such networks. There are various motivations for the recent interest in creating a

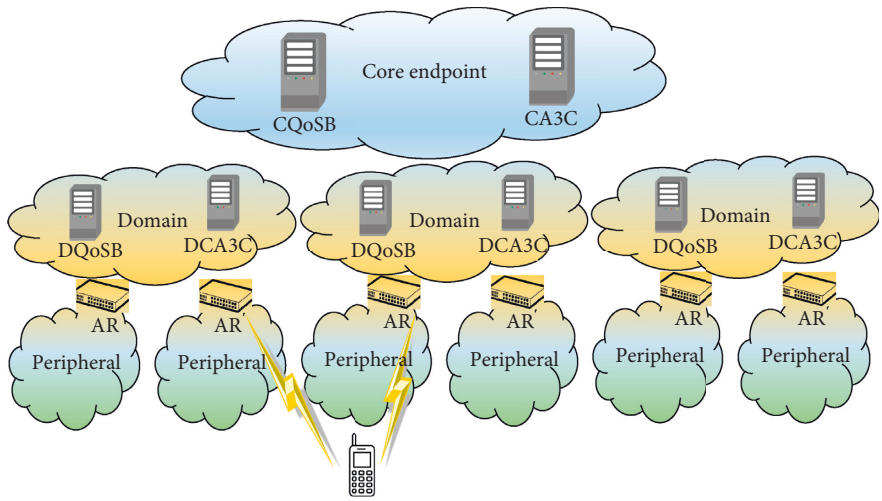

Figure 1: The core endpoint structure with the attached networks.

policy-based management system, for example, those in [18–23]:

(i) It supports the dynamic change of behaviour of the system without the need to halt. This feature suits heterogeneous network services, which should be available at all times without sudden stops or reconfiguration.

(ii) It requires less human effort to administer the network. This is an attractive characteristic when managing large-scale networks with diverse network technologies, such as 5G heterogeneous networks. Therefore, it is important to produce a policy-based system that can also be cost effective for the end user as well.

(iii) It defines the behaviour of large-scale networks or distributed systems. With a significant increase in the number of network users, the number of applications and services required by end users has grown and there is a need to define the rules of using such services and to control the relationship between different network entities. Therefore, it is a difficult task to build a management system. A policy-based management system can help to define policy rules and to enforce them.

(iv) It provides better security. Many network resources are joined in the core network, and protecting these resources from abuse is crucial. Authorised users could abuse these resources if they misuse their network privileges.

The following types of policies are used in this study.

2.4.1. Authorisation Polices. Authorisation policies specify what activities a user can (or cannot) engage in the system. Positive authorisation policies include policies that allow users access. Negative authorisation policies prohibit users from performing actions involving objects in the system [19]. Note that the use of positive and negative authorisation policies may cause conflicts. However, the policy specification language used in this study helps resolve such conflicts. We describe these conflicts and explain how to deal with them in the subsequent sections.

2.4.2. Obligation Policies. Obligation policies specify what the subject in the system must do, if a particular event occurs. Thus, predefined events trigger the security policies to execute actions. This is the basis of event condition action (ECA) rules [19]. Obligation policies have numerous applications, particularly for dealing with security violations. When a security violation occurs, a set of actions is performed to protect the network. In this study, we used such policies to deal with a predefined security violation. The set of actions is based on ITU-T recommendations, which are explained in Section 2.7. The policy specification language used in this study is Ponder2 [20], which helps the obligation policies to work in heterogeneous networks.

2.5. Policy System Selection. The variety of features policy systems such as, Ponder, PDL, XACML, LaSCO, Tower, and Ponder2 influenced the choice of an appropriate system for the working environment in this paper. The features and drawbacks of each policy were considered to determine their suitability to be part of a security management system for 5G heterogeneous networks. Although these policy systems support the main policy types needed for security management purposes, they mainly aimed to manage large distributed systems and networks, as in the case of Ponder and PDL, which are unsuitable for small devices. Ponder2 differs from PDL and Ponder in that it is more flexible and extensible, which suits environments that contain a variety of network technologies and operating systems. In addition, Ponder2 includes PonderTalk, a high-level configuration language, which ensures that the developer of a policy system does not need to know low-level details of various devices. This makes Ponder2 an ideal choice for environments that contain a range of small devices and different network technologies.

2.6. Ponder2. The Ponder2 policy system is appropriate for many environments and applications. It supports flexibility and extensibility, and provides interactivity that allows users to engage with the managed system. The most important feature of Ponder2 is being able to function with various software and hardware components and a wide range of environments, such as local area networks (LANs), wide area networks (WANs), and distributed systems [20].

According to [24], Ponder2 is implemented as a self-managed cell (SMC). An SMC is any hardware or software component capable of performing the required functions autonomously. SMCs have a self-management feature and consist of an administrative domain in the managed system. Ponder2 implements the policy-based system by considering every part in the managed system as a managed object. Managed objects can be anything, including sensors, switches, routers, and end-user devices. The concept of managed objects gives Ponder2 the seamless ability to maintain the various parts of the managed system and to utilise these components for management purposes.

Ponder2 supports both authorisation and obligation policies. Furthermore, an event type in Ponder2 is considered a managed object. An event type specifies the template to represent an event. An event is an instance of an event type and a managed object. The managed object sends a message depending on a timer or the detection of something. Moreover, Ponder2 follows the concept of domains. Domains in Ponder2 are managed objects that consist of other managed objects. The main purpose of domains is to maintain policies in an easier manner, particularly for large-scale systems. This is another capability of Ponder2 that makes it suitable for heterogeneous networks [20].

Ponder2 is a promising policy system, and it has proven to have multiple applications. It has been used in various projects at numerous institutions [22, 24] and has been implemented on different devices, including mobile phones, body sensors, and robots. The research projects in which Ponder2 has been implemented include e-health systems consisting of on-body wireless sensors [24] and self-management frameworks for unmanned autonomous vehicles [25].

2.7. International Telecommunication Union. The ITU-R offers guidelines on how to deal with certain malicious events and the actions that should be taken to protect networks. The ITU-R clearly explains that security management should follow a set of procedures after an attack occurs. We specified policies in this security management system based on these recommendations. Therefore, we focus on the ITU Telecommunication Standardisation Sector (ITU-T) recommendation M.3400 in this section.

M.3400 belongs to the telecommunications management network (TMN) group of recommendations; it provides a list of security management specifications for the TMN management function and states that security management cannot be disconnected from any telecommunication network but must be considered part of TMN management. There are groups of function sets in security management, namely, prevention, detection, containment, and recovery and security administration. We followed the specifications of security management throughout the process of designing and developing our system, and, as noted, there are several function sets. However, in our work, we investigated and utilised those best suited to achieving our security specification requirements.

We consider accessing a user's information more harmful in a Y-Comm network. Stealing user identities is becoming more of a threat in current and future mobile networks due to increased user activity on these networks. In their research study that was part of a Microsoft project investigating smart phone security, Guo et al. [26] explained about that stealing the identities of smart phone users. The danger lies in an attacker behaving like a normal user on the network after stealing the identity of a legitimate user and possibly harming the network resources. This highlights the need for a security solution as part of the network; to detect such malicious behaviour and take action to protect the network resources. In another study, [27] investigated the security of smart phones and concluded that some malicious behaviour damages not only the device itself but also network components. This situation can worsen when the attacker takes full control of the end-user device, thus generating a need for a solution incorporated into network security systems. We believe the increase of user privileges on the network due to the increasing requirements of applications increases the risk to the network associated with identity theft. An attacker who steals a user's identity may also attempt other attacks using this identity.

3. Related Work

In this section, we review the security requirements of 5G networks. Although we attempted to meet security requirements that have not been clearly met in Y-Comm security systems, the proposed security management system is extendable to achieve additional security goals. A number of techniques have been developed in 4G and 5G systems to improve data rates, including multiple-input multiple-output (MIMO) technology [28], full duplex technology [29], adaptive beamforming [28], sectorisation antennas [30], and increased capacity, latency, and QoS. Other techniques have been developed in association with the new radio access network (RAN) [30].

Regarding 5G security systems, Zheng et al. [31] explain that failing to consider devices' security in the early stage will increase the security vulnerability of 5G networks. They introduced five security requirements. Firstly, the integrity of the hardware and software of the mobile device should be protected; secondly, the security system should control access to the data stored on the mobile device. Thirdly, the integrity and confidentiality of the data stored or transported to the network operator should be protected. Fourthly, the security system should protect the users' privacy and identity. Fifthly, the security system should prevent a mobile device from being abused and used as an attack tool. The final requirement is important due to users' increased privileges in terms of network resources. In our proposed

security system, this requirement has been investigated and met. The security requirements of network operators are explained in detail in [31], and we address these requirements in the discussion of Y-Comm security systems in Section 2.1 and Section 2.2.

Different policy-based system use different mechanisms to manage the network and to provide a secure environment. However, as indicated below, the vulnerability of some related work indicates that the Y-Comm heterogeneous environment requires an improved approach.

In [32], a policy-based system is used to automatically manage security policies in a network. The system was designed and developed to reduce human involvement in network management. The system attempts to maintain security as the network changes, and it reconfigures the network if necessary. This is achieved by building an automatic management system to help the system administrators enforce policies because of the high number of changes in the network configurations and the rapid growth of network elements. Such growth makes managing the network difficult. The main component in their system is a policy engine that validates the policies and generates new configuration settings for network elements when policies are violated. However, there is a security challenge in this approach, namely, how to prevent an illegal user from gaining access to the network after the network is reconfigured. This technique is not efficient for an environment such as a Y-Comm network. As explained previously, new service providers can join the core network in Y-Comm, which makes it difficult to install a management console for each network administered. Moreover, installing more components will increase the cost of providing the services, which contradicts the security requirements of 5G networks.

In [33], authors presented a real-time transformation of authorities and dynamic aggregation between dispatched entities, which also engages with a cloud-based invocation, automatically leveraging wide levels of self-management between acting entities. However, the xml-based open standard is helping multiple actors to specify their intentions in a static objective way. Yet, the work is not reflecting clearly on critical attacks such as distributed denial-of-service (DDoS).

Lapiotis et al. [34] extended this approach and proposed a security management system focused on wireless network security issues. They presented a policy-based system architecture that includes a central policy engine, wireless domain policy managers, and local monitors. Their main motivation was the widespread use of wireless LAN, which comes with a significant increase in security risks related to malicious attacks. The researchers assumed that malicious attacks could be initiated by internal network users as well as external attackers. The system proposed by Lapiotis et al. [34] provides features such as protecting the network from new security threats without relying on the latest security mechanisms. However, one question that arises is whether the detection of abnormal traffic is sufficient in considering the demand for a highly open network. Because of the great demand in highly open heterogeneous networks to provide satisfactory services, including high-speed connections anywhere and at any time, their security management system is not suitable for heterogeneous networks. One of the limitations is that they do not indicate what kind of security policies have been enforced nor do they explain the formal validation of policies. This study follows the concept of the policy engine as the brain of the system but with numerous modifications. Furthermore, separating the policy specification from enforcement makes it more dynamic and efficient in an environment such as a Y-Comm network that contains a multilayered security service.

In [35], the authors have proposed a security management system based on an IP address supported by a spatiotemporal role-based access control (STRBAC) model. They divide a network into policy zones to improve the efficiency of policy enforcement. They addressed the numerous changes in dynamic, volatile wireless environments, including the increase in malicious attacks and the diversity of network elements. The introduction of policy zones to represent the location in their model and the role permission given to the end user to access network resources are based on these zones. Figure 2 shows the conceptual framework of the security management system based on policy zones.

The framework consists of six main components: the home agent, the foreign agent, the central authentication and role server, the local role servers, the global policy server, and the distributed wireless policy zone controllers. The local policy server is responsible for enforcing the policy in zones. However, the need for a server in each zone increases the cost and complexity of managing large and diverse networks. Additionally, the concept of dividing the network into policy zones is inefficient because legal network users access the network remotely from outside the controlled policy zones. Moreover, this approach is not scalable for wide networks or for when the current network converges with other networks. They assume that the mobile IP is always specific to a host and does not change from one location to another. This is not applicable when the network is composed of both wired and wireless technologies, such as in Y-Comm network.

In [36], the authors have detailed the security challenges (i.e., end-to-end security, tenant isolation, virtualised security, and security management) faced by 5G networks, particularly multitenant NFV/SDN-enabled 5G access networks. They have proposed a security architecture as an extension to the ETSI VNFV architecture consisting of three main components—a policy-based security management system, service monitoring and analytics systems, and VSFs to achieve the desired security functionality. The security policy manager is in charge of providing best action recommendations by taking events triggered by the service monitoring and analytics (SMA) function as input. The SMA component within the orchestration layer is responsible for performing metrics and notifications acquisition from (i) the NFVI resources, (ii) the VNFs/VSFs, and (iii) the physical infrastructure. A virtualised intrusion detection system (vIDS) or virtualised intrusion prevention system (vIPS) supported by monitoring and analytics is proposed as a security service for different 5G network services to mitigate various attacks, such as DoS. However, the cross-layer security management in 5G is not addressed.

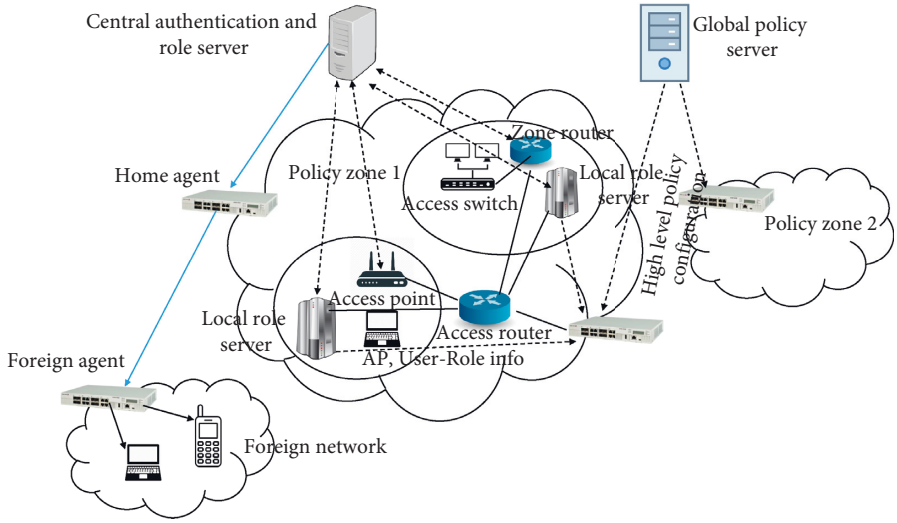

Figure 2: Wireless security management systems [35].

In [37], the authors have presented an automated SLA-driven security management framework (SEVM) for 5G networks and have implemented security services across multiple layers in 5G networks. This enables interaction between cloud service providers and tenants to detect attacks and noncompliance with security-related SLAs. Each cloud service provider has its own SEVM entity with monitoring, correlation, and remediation capabilities. Data are transferred between cloud service providers and tenants to implement security mechanisms against cyberattacks, including DDoS attacks. Events, logs, and correlated data may be exchanged in both directions based on corresponding security SLAs. The SEVM considers the interference between performance and security management and enables cloud service providers to deploy and configure security functions (e.g., firewalls and intrusion prevention systems) under strong performance requirements during the setting up of a service. The SEVM is used to automatically adjust security controls for services during runtime without violating the performance requirements of IoT applications in 5G ecosystems. For control and visibility, SEVM provides security functions (SFs) as a service to tenants, such as verticals, aimed at monitoring VMs and virtual network functions (VNFs) in slices and at correlating all relevant event and log data to detect attacks and anomalies. The SEVM monitors hyphenate SLAs from all tenants, such as security-related key performance indicators (KPIs), aimed at mitigating SLA violations before the tenants are affected.

In [15, 31, 38], the authors have investigated 5G networks and concluded that any future mobile network should meet the essential security requirements. These requirements may share characteristics of other fields in the network or distributed systems. Based on the above, we propose a security management policy-based system featuring mobile ID in the SLA stored in the core server. We enforce policing by using the current network resources without the need for more network equipment. Our system will meet the essential security requirements to provide a secure environment for users and the network, as we prove in the subsequent sections.

4. Framework Overview

As shown in Figure 3, we propose a management layer based on the ITU-T M.3400 recommendation for Y-Comm architecture. The management layer works as a security management system that is able to detect and contain predefined security violations in the network and prevent them from propagating and harming the entire network. Some detection function sets that met our requirements are as follows:

(i) The customer security alarm function set, defined as a set that supports access to a security alarm that indicates security attacks on its portion of the network and supports the detection of security violations in the network

(ii) The investigation of the ToS function set, defined as a set that supports the investigation of customers and internal users whose usage patterns indicate possible fraud or ToS and that helps recognise attacks on mobile equipment

(iii) The software intrusion audit function set, defined as a set that helps check for signs of software intrusion in the network and helps detect whether there has been a violation of the network or the mobile equipment

The M.3400 recommendations include containment and recovery function sets. One example is the exception report action function set, which supports actions to limit security breaches and provides some mechanisms. Another example is the ToS action function set, which helps limit security breaches by removing users' access privileges. We built our policies on these function sets and defined the procedures to follow if a security violation occurs. The procedures for dealing with security violations in terms of policy-based systems are explained further in the following sections.

The security requirements of 5G networks, which are explained in Section 2.3, state that the end-user device should be protected from abuse and the security system

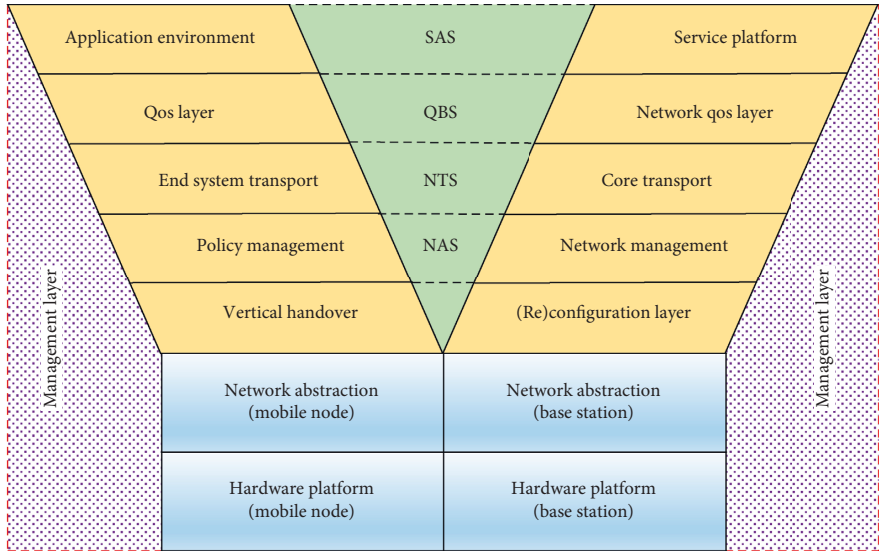

Figure 3: The complete Y-Comm architecture.

should prevent a mobile device that is under attack from being used as an attack tool. This requirement has not been satisfied in the Y-Comm architecture and needs to be addressed, as explained in Section 2.4. The opportunity to attack the network through an end-user device lies in stealing a user's network privileges. These privileges include access to sensitive data, and stealing such data triggers the security management system. The justification of considering this sensitive data is provided in Section 4.2. To detect such a security violation, we propose an intelligent agent (IA) in the end-user device. A full explanation of IA functions is given in subsequent sections.

4.1. Management Layer. The management layer is located vertically along the layers of the Y-Comm architecture. The proposed management layer, shown in Figure 3, is a policy-based system able to interact with the main components of Y-Comm. The management layer is composed of the security management system.

4.2. Security Management System. The main goal of the Security Management System is to detect attacks on the end-user device and to prevent the end-user device being used as an attacking tool. The main components of the system are the IA, security engine (SE), security administrator and security database, as illustrated in Figure 4.

The IA is located in the end-user device that works with the SE to trigger warnings when a security violation occurs. The IA has been designed to follow ITU-T recommendation M.3400. The recommendation suggests that the security management system should monitor internal users in case of ToS, as this theft can be committed with the aim of using the end-user device to attack the network resource. Thus, this important function set meets a key security requirement of 5G heterogeneous networks, which is to protect the network by preventing a legal end-user device from becoming an attack tool.

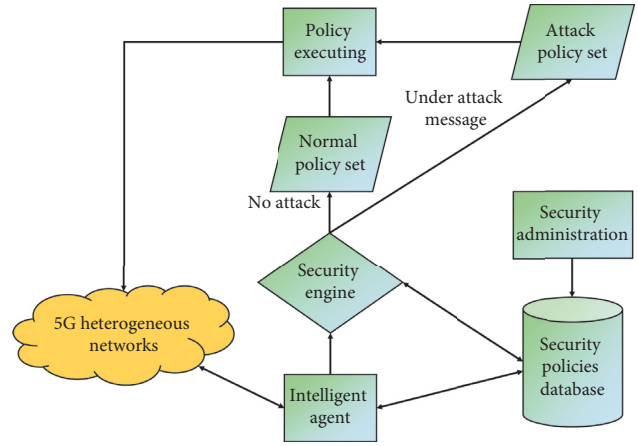

Figure 4: The proposed security management system.

The IA has four main functions:

(i) It collects related information in the end-user device based on the SE's management policies

(ii) It analyses this information and determines whether a malicious event occurred

(iii) It prepares a report and saves changes between previous and collected information

(iv) It sends the report to the SE to make a decision and apply the appropriate policy

The SE obtains information from the IA and makes a decision based on this information. This information can trigger the SE to apply the predefined security policies. In addition, the SE stores this information in the security database for future use. The SE chooses to apply the appropriate policy based on various factors: the type of attack, the type of end-user device, possible vulnerabilities in the same node, and existing records in the database. A significant threat occurs when an attacker attempts to access device configuration files to steal a user's privileges and

attack the network. Such a dangerous attack can harm the network. When the IA detects an attack, the IA warns the SE, which decides to isolate the end-user device. The isolation is based on the exception report action function set, which is part of the ITU-T recommendation, as explained in Section 2.7. The exception report action states that the security management system should limit the security breach using security mechanisms, for example, isolation. This action is taken by interacting with two main components in the Y-Comm architecture, the CA3C server and the related access router. The NLA is stored on the CA3C server, and when the SE removes a user's access privilege, the user cannot move to or access other network providers in the network. However, the user remains connected to the current service provider; therefore, the SE needs to interact with the access router to deny access and isolate the malicious device.

We designed the proposed architecture to contain a security administrator (SA) but have not implemented the SA, and we only explain its function and design factors. We believe that the SA should be automated for several reasons. First, changes in the network topology that mimic human capabilities cannot match the rapid movements in network management. Second, the functioning environment of Y-Comm is designed to allow new networks to join and other networks to extend rapidly [14]. Third, the SA needs to be automated to prevent any malicious attacks after these changes. Dynamic polices are more efficient and responsive to changes, as static policies are known to be limited [34].

4.3. Security Management Case Studies. This section describes how the system components interact in the case of a normal and a malicious event. With a normal event, no security violation or malicious behaviour occurs in the network or end-user device. Therefore, the SE does not need to take any action. However, when a security violation takes place, the IA sends a report to the SE, and the SE keeps a record in the database and executes the appropriate policy, as illustrated in Figure 5.

An end-user device is connected to the 5G heterogeneous Y-Comm network and is able to access network applications and resources; these sensitive privileges are stored as configuration files. Usually, attackers attempt to access these files with the aim of using the end-user device as a cybercrime tool. This kind of attack has occurred previously on GSM and LTE networks [26], and there is a high probability that it will happen on the 5G heterogeneous network. Such an attack will have a devastating effect due to users' increased network privileges and the openness and heterogeneity of the proposed network, as explained in Section 2.3. Our system will provide end-user devices with an IA to detect malicious behaviour and send a message to the SE that contains a mobile equipment identifier (MEID), as well as the attack type, date, and time. The SE applies and enforces the appropriate policies, in this case removing the users' access by modifying the NLA and sending a report to the current domain, which disconnects the end-user device, thus stopping the designated services. The enforcement of policies takes place at two policy-enforcement points, as discussed in Section 4.5. After the enforcement of the policies, the SE maintains a record in the database.

4.4. Policy Enforcement Points. The nature of Y-Comm architecture, based on integrating wired and wireless networks, has increased the difficulty of applying a new approach to this architecture. The security management system used in a wired network does not suit wireless networks because of the host's dynamic topology and mobility. Furthermore, the open nature of Y-Comm means that new network providers can join the core network, which leads to the need for systems that can deal with these new providers at any time. Therefore, the system we propose creates managed objects to deal with components introduced by the new network providers to enforce policies easily. These managed objects allow components to interact with the brain of the system (the SE), regardless of their configuration details. We chose Ponder2 as a tool to implement this system because it allows the creation of managed objects, which makes managing network resources an achievable task regardless of dealing with low-level equipment specifications. In addition, to support deployment of the system, the system creates adaptors using Ponder2. Adaptors in Ponder2 support deployment by allowing interaction between the heterogeneous components and the other managed objects in the system.

The Ponder2 authorisation framework (PAF) provides a way to enforce authorisation policies that can protect both the subject and the target [19] and that support negative and positive authorisation policies. However, this may introduce policy conflict, as discussed in Section 4.6. Figure 6 shows that two policy enforcement points (PEPs) are enforced in the Y-Comm architecture. The proposed security management system enforces PEP1 in the core endpoint and specifically in CA3C, which contains the NLAs. The NLAs contain the users' terms of access to the network services. Therefore, our system interacts with NLAs as managed objects to enforce the policy governing the removal of users' access to the network. This policy enforcement occurs after a security violation is detected that may harm the entire network. The end-user device needs to contact the access router, which obtains permission from the CA3C server in the core endpoint before connecting to the network. However, when removing a user's access to the CA3C server, the end-user device remains connected to the peripheral network. Therefore, another PEP is required. The second PEP is in the access router to stop providing the connection to the end-user device.

4.5. Policy Feedback Loop in the Security Management System. In this section, we discuss the application of a policy feedback loop as part of an SMC. When events trigger the proposed security management system, it analyses these events and applies the appropriate ECA obligation policy. As an extension of the obligation policy, the authorisation policy is forced back on the components of Y-Comm. This loop of interaction between Y-Comm components and the security management system is known as a policy feedback loop.

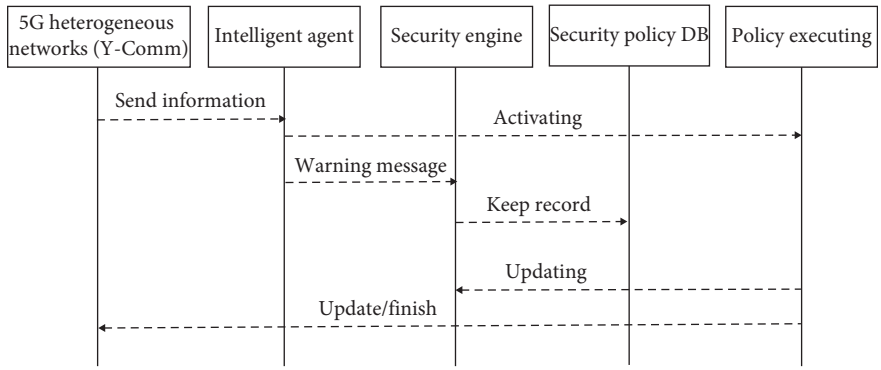

Figure 5: Sequence diagram of security management system (no security violation).

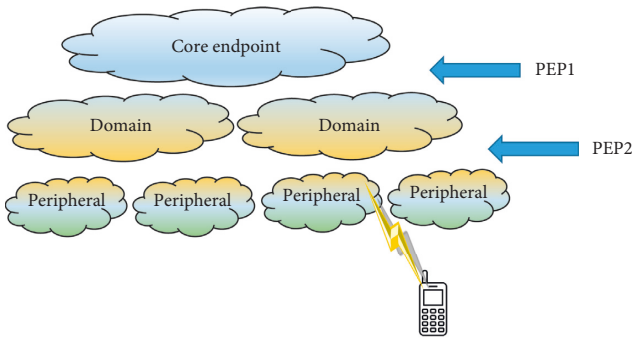

Figure 6: The policy enforcement point in the security management system.

Figure 7 shows the policy feedback loop. It illustrates the cycle of interactions between the Y-Comm network components and the proposed security management system. The Y-Comm components are managed objects, and the first managed object is the end-user device that generated events. Events are transmitted to the SE through the event bus. When the SE receives an event, it determines what decision should be taken based on the event. When the event is malicious, the system takes action based on the obligation policies. The second half of the loop is to enforce authorisation polices on managed objects in the Y-Comm network. The authorisation policies enforce two PEPs on two managed objects, the AR and CA3C. This loop represents the SMC in the system.

4.6. Resolution of Policy Conflict. Policy conflict is a common issue in policy-based systems, but Ponder2 contains features that resolve this issue when it arises in the network. Policy conflicts arise due to errors or conflicting requirements introduced by administrators. Moreover, they occur when two authorisation policies are in conflict with each other, for example, when one permits an activity and another forbids the same activity. Additionally, conflicts occur when diverse management functions apply different policies to objects in the system. Ponder2 provides a strategy for resolving policy conflict by dynamically determining which policy takes precedence. In terms of this strategy, when conflict arises between two policies, the more specific policy takes precedence. Thus, when policy $p1$ for a domain conflicts with policy $p2$ for a subdomain, $p2$ takes precedence. In the Y-Comm structure, if a conflict arises between a policy for a domain, the proposed security management system's policies are specific to a defined end-user device. For example, if a security violation takes place in the end-user device x, the IA detects and reports this violation. The SE then enforces the appropriates policy px. The policy px takes precedence because it is more specific than other polices applied to domains. The example shown in Figure 5 illustrates that the policy px conflicts with policy pa. However, the proposed security management system resolves this conflict using features of Ponder2. Therefore, in this case px takes precedence. This feature in Ponder2 is useful in the proposed security management system and meets the security requirements of 5G heterogeneous networks. Hence, this conflict resolution strategy works during runtime, which makes it more dynamic.

4.7. Specifications of the Security Management System. The approach to the proposed Security Management System is policy-based, and the system acts on two kinds of policies–obligation policies and authorisation policies. Obligation policies are specified in ECA format; thus, policies are specified to respond to events related to security violations. When an event occurs and the condition is true, action is taken to apply the appropriate policy. This integrates the security management system with the Y-Comm network. Moreover, we created managed objects for all the components needed in Y-Comm to ensure interoperability with the proposed system. Similarly, we created the components of the proposed architecture as managed objects to ensure interoperability and the achievement of the systems goals. These managed objects are the EUD, DB, AR, NLA, and the warning managed object.

Algorithm 1 explains how to create an ECA policy and how the security management system interacts with managed objects. In line (1), the system creates the ECA policy to check whether there is a security violation detected by the IA and received as an event. Then, the system receives event line (2), which contains the attributes of the attack type, EUD ID, date, and time. The condition in Ponder2 is expressed as in lines (3) and (4). The system checks whether the condition is satisfied and then activates the policy. When the ECA policy

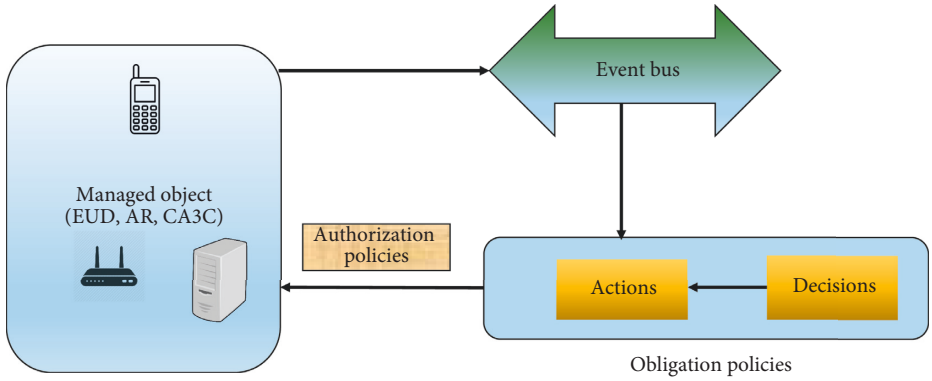

Figure 7: Security management system policy feedback loop.

(1) $Policy \longleftarrow (event, condition, attackType)$
(2) $event \longleftarrow eudValue$
(3) $condition \longleftarrow [: eudID : AttackType : Date : Time]$
(4) $attackType \longleftarrow$ "$ConfigAccess$"
(5) $print$: "$Checking\ End\ User\ Device$"
(6) $Policyaction \longleftarrow (Record, Remove\ Access, Stop\ Access, Warning, ConfigureAccess)$
(7) $Record \longleftarrow (eudID, Attack\ Type, Date, Time)$
(8) $Remove\ Access \longleftarrow eudID$
(9) $Stop\ Access \longleftarrow eudID$
(10) $Set\ Warning \longleftarrow true; show$
(11) $Configure\ Access \longleftarrow Policy$
(12) $Activate\ Policy$: $true$

Algorithm 1: ECA policy in the security management system.

is activated, the actions include four main steps. Firstly, the system keeps a record in the database and sends the four attributes to the DB managed object. Secondly, it interacts with the NLA managed objects and executes the function of revoking the user's access. In addition, it sends the EUD ID to the NLA managed object, as shown in line (7). Thirdly, the system interacts with the AR managed object to activate the function stop access, which means stop providing the service to this EUD, and sends the EUD ID. Fourthly, the system warns the system administrator of the event through the warning managed object, as shown in line (9).

Algorithm 2 illustrates the creation of an event received from the EUD managed object. The system loads the events in the event bus to interoperate with the ECA policy. The system creates the event template first and then defines the attributes of the event, as indicated in line (1), before readying the template for loading. This step is necessary to allow the ECA policy to invoke the attributes of events and check their values when an event occurs. These two algorithms show how the system employs the features of Ponder2 to deal with Y-Comm components.

5. Results

After the event generator produces random cases to test the system's ability to respond to malicious acts, the system responds to these events and enforces the required policy. The core aspect of the system is how these managed objects interoperate to achieve the security requirements. Figure 8 shows a snapshot of the system after it responds to a malicious event.

Figure 8 shows that the system performed the main steps after detecting the malicious event. It activated the policy to deny the user access and kept a record containing all details of the event. The system captures details of malicious events to allow the analysis of these events and the extension of the system. The system creates an output file to store the details of malicious events that occur in the network, as illustrated in Table 1.

As shown in Table 1, the output file contains details of the date, time and type of attack. In addition, it contains the ID of the targeted EUD in case the need arises to collect further information from the IA in the future.

6. Testing Performance

We simulate our security management system with a focus on two kind of attacks, IP spoofing and MITM attacks, which target data and control channels in 5G networks.

The system was simulated using a Mininet emulator for both attacks. As part of the setup, we considered both light and dense configuration. Light configuration with 80 nodes and dense configuration with 400 nodes, also, as a measure

(1) *template* ⟵ (*eudID*, *attackType*, *attack Date*, *attackTime*)
(2) *maliciousEvent* ⟵ *template*

Algorithm 2: Event template of the security management system.

```
run:
     [java] Shell: trying port 13570
     [java] Reading boot.p2
     [java] Reading test5.p2
     [java] Policy: active is set to true
     [java] Checking End User Device: 458X87T88 with attack type: ConfigAcs
     [java] End User Device : 458X87T88 has been denied to access the network
     [java] Keeping record of the incident in the database
     [java] ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
     [java] Checking End User Device: 359R87S98 with attack type: ConfigAcs
     [java] End User Device : 359R87S98 has been denied to access the network
     [java] Keeping record of the incident in the database
     [java] ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
     [java] Checking End User Device: 287Q9R54Y with attack type: ConfigAcs
     [java] End User Device : 287Q9R54Y has been denied to access the network
     [java] Keeping record of the incident in the database
```

Figure 8: Snapshot of the security management system after detecting a malicious event.

Table 1: Snapshot of security management system after detecting a malicious event.

EUD ID	Attack type	Data	Time
458X87T88	CONFIGACS	07/07/2019	12:24
359R87598	CONFIGACS	07/07/2019	13:43
287Q9R54Y	CONFIGACS	07/07/2019	14:14
E95T1X4W6	IPSPOOF	07/07/2019	14:54
93Q1C4E4L	CONFIGACS	08/07/2019	08:21
87W4C27YU	IPSPOOF	08/07/2019	10:05
97GKI3213	IPSPOOF	09/07/2019	10:06
96QAZ123D	CONFIGACS	09/07/2019	11:31
2DQ76XZ51	CONFIGACS	09/07/2019	13:19

of performance, the disconnect rate will be the deciding indicator. This is derived as follows:

$$r = \frac{\text{no}_{\text{ds}}}{100}, \tag{1}$$

where no_{ds} is the disconnect rate in the simulation environment. As part of the scenario, the attacker will be able to eavesdropping on the communication channel. When authentication is granted, the attacker can launch their own attacks targeting two adjacent nodes from their own device. To test various scenarios, 0 to 400 attacks were carried out and the disconnect rate was examined to test the feasibility of our system. As shown in Figure 9, the simulation results highlight that the system is robust against IP spoofing attacks. Even when the number of attacks increased to 500, the system showed proper resistance and managed to keep the disconnect rate fairly low.

As shown in Figure 10, similar to the IP spoofing, the simulation results highlight that MITM attacks are lower than 4%, showing a good level of response to such threats. In terms of performance, we can confidently state that the system fulfils the main security needs, such as availability and reliability.

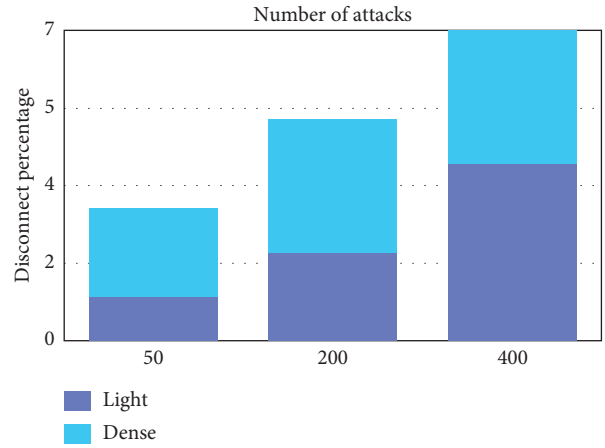

Figure 9: Performance under IP spoofing.

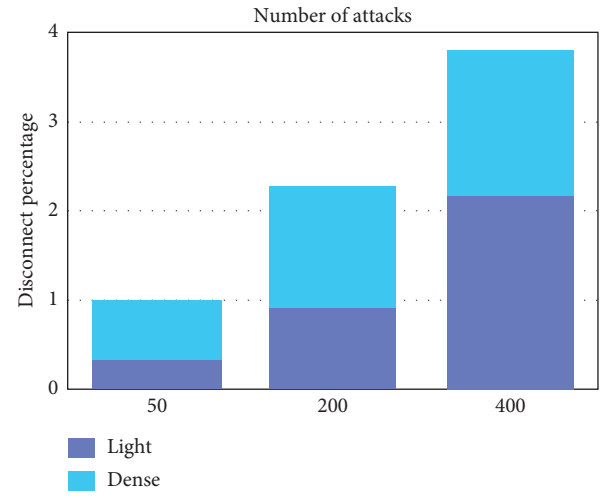

Figure 10: Performance under MITM.

7. Conclusion and Future Work

In this paper, we present an ITU-T-based Y-Comm security management network with 5G capabilities that integrates current wired and wireless networks. The main responsibility is to deliver QoS, vertical handover and heterogeneity without any major interruption of services. The results clearly demonstrate that the proposed security management system can satisfy security needs in the Y-Comm context. The deployment of the proposed system is possible with managed objects built for all components of Y-Comm using Ponder2. In addition, the system was tested against attacks, for instance, IP spoofing and MITM. The results are promising, with a low disconnection rate of less than 4% and 7%. This indicates the system is robust and reliable. The future aim is to compute

wrapping codes for components of the Y-Comm network, so they are able to interpret PonderTalk messages and complete tasks for security management purposes to propose a mechanism that gives isolated end-user devices their privileges back.

Data Availability

All data are available upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was funded by the Deanship of Scientific Research at King Saud University with grant number RG-1438-062.

References

[1] ITU, *ITU Towards "IMT for 2020 and Beyond"*, 2018, https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx.

[2] G. E. Mapp, F. Shaikh, D. Cottingham, J. Crowcroft, and J. Baliosian, "Y-Comm: a global architecture for heterogeneous networking," in *Proceedings of the 3rd International Conference on Wireless Internet; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): ICST*, pp. 22:1–22:5, Brussels, Belgium, 2007.

[3] T. Hardjono and J. Seberry, "Information security issues in mobile computing," in *Proceedings of the IFIP TC11 Eleventh International Conference on Information Security, IFIP/Sec '95*, pp. 143–151, Springer, Boston, MA, USA, 1995.

[4] Y. Park and T. Park, "A survey of security threats on 4G networks," in *Proceedings of the IEEE Globecom Workshops*, pp. 1–6, Washington, DC, USA, November 2007.

[5] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing security in 4G systems: unveiling the challenges," in *Proceedings of the Sixth Advanced International Conference on Telecommunications*, pp. 439–444, Barcelona, Spain, May 2010.

[6] H. Alquhayz, A. Al-Bayatti, and A. Platt, "Security management system for 4G heterogeneous networks," in *Proceedings of the World Congress on Engineering, WCE*, vol. 2, pp. 52–55, London, UK, July 2012.

[7] J. G. Andrews, S. Buzzi, W. Choi et al., "What will 5G Be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[8] P. Nelson, *5G and 6G Wireless Technologies Have Security Issues*, Network World, Boston, MA, USA, 2018, https://www.idginsiderpro.com/article/3315626/5g-and-6g-wireless-technologies-have-security-issues.html.

[9] A. Hammoodi, L. Audah, and M. A. Taher, "Green coexistence for 5G waveform candidates: a review," *IEEE Access*, vol. 7, pp. 10103–10126, 2019.

[10] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication," *IEEE Communications Magazine*, vol. 52, pp. 36–43, 2014.

[11] N. Tariq, M. Asim, F. Al-Obeidat et al., "The security of big data in fog-enabled IoT applications including blockchain: a survey," *Sensors*, vol. 19, 2019.

[12] T. Alexander, W. Mazurczyk, A. Mishra, and A. Perotti, "Mobile communications and networks," *IEEE Communications Magazine*, vol. 57, no. 4, p. 94, 2019.

[13] G. Mapp, F. Shaikh, M. Aiash, R. P. Vanni, M. Augusto, and E. Moreira, "Exploring efficient imperative handover mechanisms for heterogeneous wireless networks," in *Proceedings of the International Conference on Network-Based Information Systems*, pp. 286–291, Indianapolis, IN, USA, August 2009.

[14] M. Aiash, G. Mapp, A. Lasebae, R. Phan, and J. Loo, "A formally verified AKA protocol for vertical handover in heterogeneous environments using Casper/FDR," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, p. 57, 2012.

[15] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, "Security advances and challenges in 4G wireless networks," in *Proceedings of the Eighth International Conference on Privacy, Security and Trust*, pp. 62–71, Ottawa, Canada, August 2010.

[16] J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy, and L. Iftode, "Rootkits on smart phones: attacks, implications and opportunities," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems Applications*, pp. 49–54, New York, NY, USA, 2010.

[17] T. Greene, "McAfee: Android is sole target of new mobile malware in Q3," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, New York, NY, USA, 2011.

[18] J. Strassner, "Chapter 4-policy operation in a PBNM system," in *Policy-Based Network Management, the Morgan Kaufmann Series in Networking*, J. Strassner, Ed., Morgan Kaufmann, Burlington, VT, USA, 2004.

[19] K. Twidle, N. Dulay, E. Lupu, and M. Sloman, "Ponder2: a policy system for autonomous pervasive environments," in *Proceedings of the Fifth International Conference on Autonomic and Autonomous Systems*, pp. 330–335, Valencia, Spain, April 2009.

[20] J. Zhou, Q. Shen, and Y. Xu, "Research and improvement of Ponder2 policy language," in *Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, vol. 2, pp. 455–458, Zhangjiajie, China, May 2012.

[21] R. Neisse, P. D. Costa, M. Wegdam, and M. Sinderen, "An information model and architecture for context-aware management domains," in *Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks*, pp. 162–169, Palisades, NY, USA, June 2008.

[22] H. Zhao, J. Lobo, and S. M. Bellovin, "An algebra for integration and analysis of Ponder2 policies," in *Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks*, pp. 74–77, Palisades, NY, USA, June 2008.

[23] M. Asim, A. Yautsiukhin, A. D. Brucker, T. Baker, Q. Shi, and B. Lempereur, "Security policy monitoring of BPMN-based service compositions," *Journal of Software: Evolution and Process*, vol. 30, no. 9, Article ID e1944, 2018.

[24] E. Lupu, N. Dulay, M. Sloman et al., "AMUSE: autonomic management of ubiquitous e-Health systems," *Concurrency and Computation: Practice and Experience*, vol. 20, no. 3, pp. 277–295, 2008.

[25] E. Asmare and M. Sloman, "Self-management framework for unmanned autonomous vehicles," in *Proceedings of the 1st International Conference on Autonomous Infrastructure, Management and Security: Inter-Domain Management*,

pp. 164–167, Springer-Verlag, Berlin, Heidelberg, Germany, 2007.

[26] C. Guo, J. Helen, and W. Z. Wang, *Smart-Phone Attacks and Defenses, HotNeT III*, 2004.

[27] S. Töyssy and M. Helenius, "About malicious software in smartphones," *Journal in Computer Virology*, vol. 2, no. 2, pp. 109–119, 2006.

[28] F. W. Vook, A. Ghosh, and T. A. Thomas, "MIMO and beamforming solutions for 5G technology," in *Proceedings of the IEEE MTT-S International Microwave Symposium (IMS2014)*, pp. 1–4, Tampa, FL, USA, June 2014.

[29] S. Goyal, P. Liu, S. S. Panwar, R. A. Difazio, R. Yang, and E. Bala, "Full duplex cellular systems: will doubling interference prevent doubling capacity?," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 121–127, 2015.

[30] H. Kim, I. Jung, Y. Park, W. Chung, S. Choi, and D. Hong, "Time spread-windowed OFDM for spectral efficiency improvement," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 696–699, 2018.

[31] Y. Zheng, D. He, W. Yu, and X. Tang, "Trusted computing-based security architecture for 4G mobile networks," in *Proceedings of the Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05)*, pp. 251–255, Dalian, China, December 2005.

[32] J. Burns, A. Cheng, P. Gurung et al., "Automatic management of network security policy," in *Proceedings of the DARPA Information Survivability Conference and Exposition II. DISCEX'01*, vol. 2, pp. 12–26, Anaheim, CA, USA, June 2001.

[33] Y. Karam, T. Baker, and A. Taleb-Bendiab, "Security support for intention driven elastic cloud computing," in *Proceedings of the Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation*, pp. 67–73, Malta, November 2012.

[34] G. Lapiotis, S. Das, and F. Anjum, "A policy-based approach to wireless LAN security management," in *Proceedings of the Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, pp. 181–189, Athens, Greece, September 2005.

[35] S. Maity, P. Bera, and S. K. Ghosh, "A mobile IP based WLAN security management framework with reconfigurable hardware acceleration," in *Proceedings of the 3rd International Conference on Security of Information and Networks*, pp. 218–223, New York, NY, USA, 2010.

[36] M. S. Siddiqui, E. Escalona, E. Trouva et al., "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks," in *Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 44–49, Palo Alto, CA, USA, November 2016.

[37] I. Adam and J. Ping, "Framework for security event management in 5G," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 51: 1–51:7, New York, NY, USA, 2018.

[38] K. H. Y. uk Yu Hui, "Challenges in the migration to 4G mobile systems," *IEEE Communications Magazine*, vol. 41, pp. 54–59, 2003.