Intrusion detection techniques for mobile cloud computing in heterogeneous 5G

Keke Gai, Meikang Qiu*, Lixin Tao and Yongxin Zhu

ABSTRACT

Mobile cloud computing is applied in multiple industries to obtain cloud-based services by leveraging mobile technologies. With the development of the wireless networks, defending threats from wireless communications have been playing a remarkable role in the Web security domain. Intrusion detection system (IDS) is an efficient approach for protecting wireless communications in the Fifth Generation (5G) context. In this paper, we identify and summarize the main techniques being implemented in IDSs and mobile cloud computing with an analysis of the challenges for each technique. Addressing the security issue, we propose a higher level framework of implementing secure mobile cloud computing by adopting IDS techniques for applying mobile cloud-based solutions in 5G networks. On the basis of the reviews and synthesis, we conclude that the implementation of mobile cloud computing can be secured by the proposed framework because it will provide well-protected Web services and adaptable IDSs in the complicated heterogeneous 5G environment. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS
intrusion detection; mobile cloud computing; security; heterogeneous 5G

*Correspondence
Meikang Qiu, Department of Computer Science, Pace University, New York, NY, 10038, U.S.A.
E-mail: mqiu@pace.edu

1. INTRODUCTION

The recent rapid development of the advanced mobile technologies has resulted in a great jump for the growth of mobile cloud computing (MCC) [1,2]. The core benefit of adopting MCC is to improve the performance of mobile devices by integrating three Internet-related technologies [3], involving mobile computing, mobile Internet, and cloud computing. Considering the Fifth Generation (5G) context in the near future, MCC will have higher level performances in offloading computations by migrating data processing and data storage to the cloud for improving mobile devices’ capacities [4–7] by the reason of enhanced bandwidth. However, the advanced wireless networks will face many challenges in security domain [8,9], which has been explored by prior research from various perspectives [10]. One of the challenges is that overcoming hazards from intrusions is difficult because of high efficiency wireless communications, mutual interferences between signal cells, improper user authentications, managing tool limitations, and intentional attacks. Advanced networking speed may assist attackers to hide their intrusions.

This paper addresses security issues in MCC and synthesizes recent achievements in intrusion detection techniques in order to find the approaches that can effectively utilize the advances of heterogeneous 5G. In the domain of wireless security, preventing wireless communications from intrusions is a vital part. The intrusion detection-based approach is considered as an approach providing secure communication environment for future networks.

As a traditional security approach, intrusion detection system (IDS) is a dynamic discipline that has been associated with diverse techniques. With the distinct features of each technique, each detection method has both predominance and limitations. The significance of being aware of IDSs is that it is a fundamental of generating future optimized models for securing MCC-based services in 5G.

The main contributions of this paper are twofold:

- It provides future 5G developers and users with a logical effective model to achieve secure data transmission in MCC by applying IDSs.
- It reviews and synthesizes all crucial security concerns in MCC from a technical perspective.
Intrusion detection techniques for mobile cloud

The rest of this paper is structured as follows. Section 2 provides an overview of MCC terminology in 5G and three aspects addressing mobile computing, mobile Internet, and technologies behind cloud computing. Section 3 gives a summary of IDSs with a review of its key technologies. In Section 4, we give a discussion with a number of future research suggestions. And the conclusion is drawn in Section 5.

2. MOBILE CLOUD COMPUTING TERMINOLOGY IN FIFTH GENERATION

2.1. Mobile cloud computing

Mobile cloud computing is a paradigm integrating mobile computing and mobile Internet with cloud computing for the purpose of acquiring cloud-based services in the mobile environment [11–14]. One of the crucial features of this mobile model is that both data storage and data processing are migrated to the cloud from mobile devices [15]. With the migration of data storage and data processing, MCC model is designed to support applications running in the cloud that offer higher-level centralized functions [16]. Considering security concerns in MCC, the threats’ assessment can address security problems from three constituent technologies, namely, mobile computing, mobile Internet, and cloud computing.

Figure 1 represents a technique structure model for MCC, which illustrates main techniques being deployed in the current industry. For example, three key techniques supporting cloud computing include parallel programming model, virtualization, and mass distributed storage. The following subsections give detailed information concerning three fundamental technologies in MCC.

2.1.1. Mobile computing

The term mobile computing refers to the platform supported by wireless networks that enable portable devices to access services on the Web [11,17]. The platform in mobile computing is the manner for end users to acquire Web services in the wireless environment. The main advantage of leveraging mobile computing is to reduce applications’ development time [18].

However, mobile computing relies on wireless technology and faces threats when communications take place via wireless networks, although it is often restricted by hardware capacities [19]. For example, one of the threats of mobile computing [20] is that the wireless communications can be easily invaded when using virtual private network because of the interconnecting various networks. The security level usually depends on the authentication means and encryption method for virtual private network access.

2.1.2. Mobile Internet

The mobile Internet is an advanced networking technology derived from the development of wireless networks. Current active technologies include WiFi, Third Generation (3G), and long-term evolution [21]. 5G is considered as the future acquisition for mobile Internet. The core concept of mobile Internet is connecting two communicators via wireless networks and supporting Web-based applications, which can be also defined as Web services.

The term Web services [22,23] refers to the integrations of Web-based applications by using Extensible Markup Language (XML); Simple Object Access Protocol (SOAP); Web Services Description Language (WSDL); and Universal Description, Discovery, and Integration (UDDI). The integration provides electronic devices with a networking-based communication approach.

In a perspective of mobile Internet, security concerns often address service layer objects, such as [24] platform, application, and infrastructure layers, because the security criteria and requirements maybe varied. Nevertheless, no matter which service layer is concentrated, the wireless network itself always faces threats from intrusions.

2.1.3. Behind cloud computing

The technologies supporting cloud computing are very similar regardless of service types or deployments [25,26]. We summarize three current operative technologies for adopting cloud computing, including the virtualization, mass distributed storage (MDS), and parallel programming model (PPM) technologies [27–30].

First, virtualization is a service deployment approach that is broadly used in cloud computing. The main purpose of the virtualization is to divide computing resources into various service levels [28,31] by virtualizing object resources, such as data, servers, networks, and physical machines [30]. Once the service levels are categorized, services are delivered by virtual machine (VM).

A VM in cloud computing is an approach of allocating computing resources to a group of logic-related entities [32–34] and representing information to end users. It is an isolate application running on the operating system that provides end users with a virtualized functionality. The prime motivations of using VMs [35] are reducing costs, saving energy [36,37], and simplifying maintenance.
Moreover, VMs can protect end users’ information because of the platform independency [38,39], which means that VMs are isolated from other components of the system. In a networking context, attackers can only gain controls on VMs by attacking the lower layer hypervisor [40]. Nevertheless, the greatest vulnerability in using VMs is that it is hard to maintain a consistent security because of its dynamic nature [41]. Migrating VMs among physical servers can result in security risks because there is no firewall segregating VMs within a virtual operating environment.

Other concerns when adopting VMs include virtualization overhead and reliability [42]. To address these issues, Lin et al. [43] proposed an approach that supported hardware-assisted virtualization, which was termed as hybrid virtualization (HV).

Second, MDS technology [30,44,45] is a manner of increasing data reliability and infrastructre credibility by adopting multiple storage servers and applications. This approach can avoid losing data from site disasters because data are stored in different places. The interconnections between heterogeneous networks can seamlessly connect distributed services in MCC [46]. However, the security concern is that unreliable storage devices may be used as a unsaty infrastructure for users. Wireless traffics among different physical locations can lead more chances of intrusions. In an intensive networking environment [46], this technique may cause services discontinuity, signals interruptions, and networking management chaos. One solution to MDS technology [46] is providing transparent cloud-base services for end users.

Finally, the PPM technology [30,47] is termed as a cloud-based solution supporting synchornous tasks. This technology is widely used in parallel data processing by adopting parallel programming applications [47,48] that drill down tasks into a number of subtasks. It is also considered as an efficient approach of solving large-size data transmissions [48].

In summary, technologies behind cloud computing are fundamentals of our model, which are aligned with both security concerns and solutions. The following section reviews the concept of heterogeneous network that provides networking platform for cloud computing.

### 2.2. Heterogeneous Fifth Generation networks

A heterogeneous wireless network describes an integrated network that connect end users’ portal devices with various operating systems or protocols without restrictions of manufacturers. This mixture-style network is a trend in the advanced wireless era that supports Mobile Broadband services [49]. The desired high compatibility and performance supported by applying new spectrums is a fashionable expectation. However, current methods of allocating spectrum need to take a long term to reach this expected goal [50].

Considering current performances of heterogeneous networks, some predictable features of future heterogeneous 5G can be determined within a mobile cloud context. The first expectation is that heterogeneous 5G can enhance future devices’ performances. For example, mobile cloud-based heterogeneous networking solutions provide end users with a means of managing performance and energy consumption trade-off [51]. Leveraging distributed-based approaches will be implemented more broadly because the capacity of 5G dramatically increases.

However, there are a number of concerns regarding security. For instance, heterogeneous wireless networks allow end users to easily switch networks between WiFi and Fourth Generation (4G) and 5G, which leads to the concerns of interoperability [52]. Lack of standardized radio access may cause massive interferences for adopting MCC, where it may provide attackers with intrusion opportunities. The following section reviews current active or novel intrusion detection approaches in the advanced wireless context.

### 3. INTRUSION DETECTION SYSTEMS

An IDS is a monitoring infrastructure or application that surveils all events or communication traffic taking place in a computing system or over networks and generates reports to the management system by differentiating intrusions, suspicious activities, and other malicious behaviors [41,53–55]. The term intrusion, also known as attack, is a behavior of evading computer security policy or standard [56,57], which can occur in various situations [58].

In a wireless networking environment, the IDS usually focuses on observing the processes of wireless communications and examining the behaviors and activities represented in the processes. Considering the methods of data collection, there are two sorts of IDSs [58], namely, host-based IDS and network-based IDS. A host-based IDS collects data from specific system log files running on the node. Instead, a network-based IDS gathers data by surveilling and capturing the traffic.

Moreover, from a perspective of techniques, network-based IDSs can be grouped into five basic categories, including signature-based detection (SBD), anomaly-based detection (ABD), specification-based detection (SPBD), stateful protocol analysis detection (SPAD), and hybrid intrusion detection. Figure 2 represents a technique model for IDSs with key characteristics of each technique.

### 3.1. Detection methodologies

This section reviews the concepts, deployments, limitations, and techniques of diverse IDSs, including the SBD, ABD, SPBD, SPAD, and hybrid intrusion detection approaches. Table I displays these approaches’ principles, performances, and limitations.
Intrusion detection techniques for mobile cloud

K. Gai et al.

Figure 2. Techniques model for intrusion detection systems.

Table 1. Comparisons of different intrusion detection approaches.

<table>
<thead>
<tr>
<th>Methodologies</th>
<th>Principle</th>
<th>Performance</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBD</td>
<td>Seeking</td>
<td>Rely on the pre-installed intrusion signatures databases that are used to compare the network traffics with the stored signatures at database</td>
<td>Common limitations of SBD include 1. Limited ability to deal with new threats and encrypted packets, 2. An excess network packet can cause performance deductions, 3. Inefficient supports for weak authorizations</td>
</tr>
<tr>
<td>ABD</td>
<td>Monitoring</td>
<td>Supported by three techniques, including statistical-based, knowledge-based, and machine learning-based ABD.</td>
<td>Different techniques may cause various risks. Two common challenges are as follows: 1. Building a precise normal profile is difficult, 2. Defining parameters and criterion is difficult</td>
</tr>
<tr>
<td>SPBD</td>
<td>Behavior</td>
<td>Examine the variable-length patterns for detecting new threats or attacks with lower level false positive</td>
<td>The type of techniques depends on the demands.</td>
</tr>
<tr>
<td>SPAD</td>
<td>Separate</td>
<td>Evaluate both TCP and UDP; Provide stateful characteristics protocol analysis</td>
<td>Two restrictions for deploying SPBD involve: 1. A great workload of defining normal behavioral specifications, 2. Novel attacks or threats can be only detected while the risks physically occur in most situations</td>
</tr>
<tr>
<td>HID</td>
<td>Simultaneously deploy multiple detection methodologies</td>
<td>Have a chance to gain advantages from the combination in order to deal with advanced requirements or complicated traffics</td>
<td>Two major limitations are as follows: 1. Highly rely on the protocol analysis request or response, 2. Cannot detect intrusions based on the single protocol analysis</td>
</tr>
</tbody>
</table>

SBD, Signature-based; ABD, anomaly-based; SPBD, specification-based; SPAD, stateful protocol analysis; TCP, Transmission Control Protocol; UDP, User Datagram Protocol; HID, hybrid intrusion detection.

3.1.1. Signature-based detection and approach.

An SBD is a widely acceptable approach for antivirus software to identify malware by looking into malware signature. The term signature refers to the pattern or string correlating with the known threatening interventions [41]. The process of SBD relies on the pre-installed intrusion patterns or strings on the database. This operating manner limits its performance because the malware signature will not be detected when the SDB system is not updated. The IDS using SBD may not be able to identify the new threats when the system connects to the Internet because the intrusions are dynamic.
This restriction can be partially solved by deploying an automated signature creator attached to the SDB systems [59,60]. The signature creator can be generated from collecting and analyzing constituents of frequent or consistent behaviors [60,61]. However, the limitation of this solution is that current algorithms cannot fully detect all malicious instances. Most approaches addressing this issue determine the suspicious traffic by analyzing the data streams’ reflections [61], which cannot entirely secure the outcomes.

In addition, an excess of network packet often causes the performance deductions when the processing capability cannot match the wireless transmission ability [62]. This situation can be improved by migrating data processing and storage to the cloud and examining the parallel exclusive signature matching on the cloud-based servers [63]. Through the analysis among parallel data transmissions between end users and cloud-based servers, the cloud-based SBD system can achieve intrusion detection without network packet overload.

3.1.2. Anomaly-based detection and approach.

The ABD system refers to an approach of identifying apparent divergences or inconsistencies between the target events and predefined normal transmissions [62,64–66]. The comparison can determine whether there is a partition between normal and unusual behaviors, and the unusual behavior is considered as an active or potential attack, which depends on the level of differences. Three common techniques [67] supporting comparisons include statistical-based [68], knowledge-based, and machine learning-based techniques [69,70].

Statistical-based technique tracks all networking traffics and generates a profile examining whether there are any improper traffic by a statistical analysis [67]. The statistics are formulated by evaluating the correlations among the defined parameters, such as ports and devices, traffic rates, packets connecting to each protocol, and Internet Protocol addresses. The difficulties for applying statistical-based technique are twofold. First, positioning a proper balance between positive and negative behaviors is hard. Second, this technique may fail when the system is being attacked.

Next, the knowledge-based technique is applicable for those systems that consist of specific knowledge structures or attached to a set of rules [67], such as symbolic representations. The rules are composed of features and classes, which can be generated by experts or testing approaches. The gathered data are categorized and allocated into different rules. The limitation of this technique is that formulating quality knowledge-based rules can suffer a prolonged development.

Finally, a machine learning-based technique [70,71] is a procedure of constructing new behavior models based on the observations of activities, events, and behaviors. The means of data analysis is similar to statistical-based technique. The difference is that the machine learning-based technique can acquire new information model based on the analysis [72]. The obstacle of adopting this technique is the extensive requirement of computing resources [67], which imply that the examination is highly dependent on the stored secure behavior assumptions.

In summary, the main challenges of ABD system include the following: (i) building a precise normal profile is burdensome for the reason of the traffic variety and dynamic networking environment [73]; and (ii) defining parameters and criterion is tough because attackers can be trained in evading the apparent symptoms [70].


Compared with ABD, an SPBD has a similar mode for detecting deviations but needs users to establish a behavior evaluation standard in a special-dynamics formation [74]. The motivations of applying an SPBD system are to obtain higher level capabilities in detecting new attacks and increasing accuracy. An SPBD approach is considered as an appropriate solution to examining the variable-length patterns [75]. However, similar to other ABD systems, an SPBD system also requires a great workload of defining normal behavioral specifications.

3.1.4. Stateful protocol analysis and approach.

The SPAD is a novel approach of intrusion detection that distinguishes irregular events from routine streams in a session by leveraging a pre-determined ubiquitous profile [76]. The profile provides end users with a list of secure and trustworthy activity definitions. Both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) will be evaluated when performing the SPAD [77]. The main positive feature of this technique is providing protocol analysis with stateful characteristics.

Despite that the SPAD offers strong protocol analyses, there are two limitations in practice. First of all, this technique highly relies on the protocol analysis so that attackers can avoid intruding the general accepted protocol characteristics in order to deceive the SPAD into believing that the system is secure [78]. Moreover, this technique does not completely solve the problem of detecting attacks based on a single request or response. Addressing this problem, more stateful characteristics need to be added to the protocol analysis profile, which synchronously causes heavy workloads and oversized packets.

3.1.5. Hybrid intrusion detections.

Multiple intrusion detection approaches can be simultaneously deployed based on the security demands [71,74,79,80]. The purpose of combining two or more techniques is to design new intrusion processes by taking advantages of different techniques. For example [80], combining ABD with Knowledge-based Intrusion Detection (KBD) has been proved that it can protect mobile ad hoc networks from a range of attacks. Moreover, it also has been examined that integrating SPBD with ABD can enable the specification-based detection approaches to take
advantage of machine-learning algorithm, which assists the SPBD system to obtain the ability of creating new patterns [74].

The main challenge of this approach is that effectively combining multiple detection means is difficult. The balance point of workload, efficiency, and security is hard to position. Because two or more detection manners work together, the packet overhead is hard to be avoided.

### 3.2. User authentication

In MCC, a password cannot match the security requirements for an access authentication in those industries that require higher level security. A number of approaches for generating strong user authentications have been created. The purpose of the authentication [81] is to verify users’ identities by leveraging effective authentication mechanisms to ensure that the access requests are sent by the parties with proper authorizations.

An important mechanism category is biometric authentication that examines users by identifying individual features [82–85], such as physical characteristics and behaviors [86]. This approach is a complementary support for password-based verifications, which can provide a secure end users access. Nevertheless, this technique delivers personal information and uses the data as the accesses to the authentication systems. Any intrusions during the wireless communications can cause threats to personal privacy.

### 4. DISCUSSIONS

According to the aforementioned reviews, the implementation of MCC within a heterogeneous 5G network provides end users with many potential expected features, such as faster bandwidth. The new feature will bring users positive user experiences as well as potential risks including security concerns. For achieving a secured networking environment, installing an IDS is able to increase the security level of mobile devices, albeit this approach is restricted by the current networks performance.

In order to address this issue, we propose a high level framework of leveraging MCC-based IDSs for protecting mobile application utilizations that are explicated in Figure 3. In this framework, all data transmissions are delivered by the heterogeneous 5G networks, which signify the flexibility of networking choices for mobile users. All data processing required by intrusion detections are migrated into cloud. Previous research has provided a variety of approaches for achieving secure networking environment by adopting energy-aware security algorithm or embedded systems [9,87].

For a current typical cloud-based application, generating private key and public key in most situations can only protect the data transmissions. The reason of this phenomenon is that the restriction of networking bandwidth cannot support effective protections offered by the third party in the cloud. Otherwise, mobile devices may face challenges in energy loss and long latency.

Fortunately, the proposed framework highlights the advantages of heterogeneous 5G and combines cloud-based IDSs with other applications in the cloud. The widened bandwidth provides an effective networking platform that can give strong supports to the intrusion detection activities. The IDSs interface running on mobile devices can implement a background operation that is responsible for traffic data collection. The normal profile database and dynamic machine-learning system in

![Figure 3. High level framework of leveraging MCC-based IDSs on mobile applications.](image-url)
the cloud can offer capable functions and performances as the cloud-based data processing has less concerns on power consumptions and storage. It is possible to develop a functional IDS that consists of a full set of profile packages.

5. CONCLUSIONS AND FUTURE WORK

Being productions of networking technologies, MCC and heterogeneous 5G are desired to bring users more benefits. Nonetheless, wireless communications will not be secured unless the data transmissions are protected by an efficient approach. This paper reviewed essential concepts and recent research achievements about MCC, heterogeneous 5G, and IDSs. Based on the outcomes of the review, we proposed a high level framework that uses cloud-based intrusion detection approach to gain a secure wireless communication in 5G.

Moreover, we proposed a number of questions for future research.

(1) How can we prevent users’ privacy leaks when adopting the cloud-based IDS? (2) What is a secure data transmission method between end users and cloud-based IDSs? (3) Whether we can develop an energy-aware model for mobile devices in order to ensure they can fully utilize the benefits of heterogeneous 5G.

ACKNOWLEDGEMENT

This work was supported in part by the National Science Foundation under Grant numbers CNS-1457506 and CNS-1359557.

REFERENCES

Intrusion detection techniques for mobile cloud

K. Gai et al.

Conference on Future Networks and Communications (FNC’14)/The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC’14)/Affiliated Workshops, Niagara Falls, Ontario, Canada, 2014; 434–441.


Intrusion detection techniques for mobile cloud


