A Method of Fraud & Intrusion Detection for E-payment Systems in Mobile e-Commerce *

Pallapa Venkataram, B.Sathish Babu, Naveen M.K., and Samyama Gungal G.H.
Protocol Engineering and Technology Unit, Electrical Communication Engineering,
Indian Institute of Science, Bangalore-560 012, India
E-mail:{pallapa,bsb}@ece.iisc.ernet.in, {naveen,samyama}@protocol.ece.iisc.ernet.in

Abstract

The need for paying with mobile devices has urged the development of payment systems for mobile electronic commerce. In this paper we have considered two important abuses in electronic payments systems for detection. The fraud, which is an intentional deception accomplished to secure an unfair gain, and an intrusion which are any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. Most of the available fraud and intrusion detection systems for e-payments are specific to the systems where they have been incorporated. This paper proposes a generic model called as Activity-Event-Symptoms(AES) model for detecting fraud and intrusion attacks which appears during payment process in the mobile commerce environment. The AES model is designed to identify the symptoms of fraud and intrusions by observing various events/transactions occurs during mobile commerce activity. The symptoms identification is followed by computing the suspicion factors for event attributes, and the certainty factor for a fraud and intrusion is generated using these suspicion factors. We have tested the proposed system by conducting various case studies, on the in-house established mobile commerce environment over wired and wire-less networks test bed.

Keywords: mobile commerce, security, intrusion, fraud, transactions

1. Introduction

Mobile Commerce is a Commerce brought to mobile users via mobile devices such as laptops, palmtops, PDA's or most dominantly mobile phones. With an ever increasing number of devices in the market, mobile phones will undoubtedly play a crucial role in promoting the mobile Commerce [7]. M-commerce enables electronic transactions or information interactions conducted using a mobile device and mobile networks. M-commerce involves m-payment, which is defined as the process of two parties exchanging financial value using a mobile device in return for goods or services [5]. The various actors which are involved in mobile payment process are: *Consumer,* who owns the mobile device and is willing to pay for a service or product trough some payment provider; *Content provider or merchant,* who sells product to the customer; and the *Payment service provider,* who is responsible for controlling the flow of transaction between mobile consumers, content providers and trusted third party(TTP).

Payment transaction process in a mobile environment is very similar to typical payment card transaction. The only difference is that the transport of payment details involves wireless service provider, use of WAP/HTML based browser protocol or bluetooth and infrared technologies. Following are the main steps in Mobile payment life cycle: 1. Customer opens an account with payment service provider for payment service through a particular payment method. 2. Customer indicates the desire to purchase a content using a mobile device. 3. Content provider forwards the request to the payment service provider. 4. Payment service provider then requests the TTP for authentication and authorization and informs content provider about the status of the authentication and authorization. 5. On successful authentication of the customer, the content provider will deliver the purchased content. 6. Payment settlement will take place in real-time, prepaid or postpaid mode.

1.1. M-Payment solutions

This section will portray some of the current mobile payment solutions. The Electronic Payment Systems Observatory (ePSO) identified over 30 different mobile payment solutions, each with its own particular set of technologies. Mobile operators provide many solutions, some by financial players and others involving alliances between opera-

*Research grant courtesy: Ministry of Information Technology, Government of India.

tors and financial organizations. Existing mobile payment solutions are categorized based on the payment settlement methods into: *prepaid,* using smart cards or digital wallet; *instant paid,* by direct debiting or off-line payments; and *post paid,* through credit card or telephone bill. The three payment settlement options may vary in their requirements, process of payment and technologies used. The only requirement to a prepaid type of payment solution is a PIN for authorizing a transaction and a smart card value or stored value card for making payment. Some of the mobile payment solutions are: *Paybox, Paypal, m-Pay, iPIN, Netpay, Paybill, Jalda*.

1.2. Security challenges in Mobile payment systems

The m-commerce security challenges relate to the user's mobile device, the wireless access network, the wired-line backbone network, and m-commerce applications. Security threats in m-commerce may be passive (such as information monitoring and release for fraudulent purposes) or active (such as the modification of information through denial-of-service and unauthorized access). Fraud is an intentional deception or misrepresentation that an individual knows to be false or does not believe to be true makes, knowing that the deception could result in some unauthorized benefit to himself/herself or some other person. The frauds that can occur in the m-commerce environment have been categorized as mobile phone fraud, mobile network fraud and fraud specific to the mCommerce transaction process. Some of the frauds specific to e-payment systems are [2]: *Merchant Fraud; Customer Fraud; Third Party Fraud; etc.* An intrusion is all inbound and outbound network and user activity with suspicious patterns that may indicate a network or a system attack from someone attempting to break into or compromise a system [3]. Some of the intrusions happen in mobile commerce environment are: Attempts from the competitors; Attempts to get unauthorized entry into customer private accounts; Attempts to spoil the reputation of the vendor; etc.

1.3. Proposed transaction based IFDS

The intrusion and fraud detection systems(IFDS) which are designed for electronic commerce can not be directly applied to mobile commerce environment; due to location dependency, ubiquitous operation and choice of heterogeneous mobile devices to perform the mobile commerce transactions. In this paper we propose an AES model for fraud and intrusion detection system for payment systems in mobile commerce environment. We are presenting the functioning of system with respect to customer where the intruder performs an account takeover attack by stealing the identity of a genuine customer and using that account he/she commits third party fraud. The AES model effectively identifies this fraud in real time based on generated symptoms.

1.4. Organization of rest of the paper

The rest of the paper is organized as follows, section 2 gives information about some of the related works, section 3 gives some of the definitions, terminologies and concepts used in the paper, section 4 discuss the proposed method in detail, section 5 illustrates simulation with results, and finally, section 6 draws conclusion.

2. Related Works

We are presenting few works, related to detection of frauds in cellular networks. The Adaptive fraud detection [4], proposes a method to detect cellular cloning fraud based on database of call records. A rule learning program is used to generate parameters of fraudulent behavior from customer transactions database. The drawbacks of the method are time consumption during neural network training and the method detects only learned attacks. A signature-based system has been proposed in [1], this system is event-driven rather than time driven so that fraud can be detected as it is happening and not at fixed intervals of time. It is based on the concept of account signatures which may describe call durations, time lapse between the calls, days in a week and certain times of day, terminating numbers, and payment methods for the particular account. Host based intrusion detection system [6], based on users signatures, proposes developing precise user signatures characterizing multiple aspects of user activity. It assumes that each user has a sequence of commands that they frequently type in. The probabilistic state finite automata is constructed using these command traces. Based on the current activity initiated the probabilities are updated using standard deviation approach. The method is more specific to users commands analysis instead of activity analysis, which is very much essential for commerce environment.

3 Definitions

In this section we provide some of the definitions, nomenclatures and concepts used in the paper.

Mobile Commerce Service Provider(MCSP)

In the proposed system MCSP is assumed to offer the following services to mobile commerce customer: *Identifies the genuine vendors who offers mobile commerce service; Maintains vendors index ; Periodically updates the vendor index; Ranking the vendor; Provides vendor details to genuine customers on a request; etc.*

Detection Support System(DSS)

The Detection Support System (DSS) works like a gateway for other entities to access IFDS. It receives detection requests from various actors of mobile commerce environment. The request is passed onto IFDS for analysis, further the response of IFDS will be sent back to requesting entity. The DSS also assists in creation and maintenance of various databases used by IFDS.

Activity database

An activity here refers to a set of related tasks which will be executed during the business transaction. The activity database is used to store the set of identified activities of the Mobile Commerce. Every activity is identified using an activity identifier A_i, and an event under an activity is identified using event identifier E_{ij}. e.g.: For a Mobile Shopping activity, the events could be: *Vendor selection; Product selection; Placing purchase order; Providing payment details; Providing shipment details; etc.*

Event

An event is an occurrence in a business transaction to which that business must respond. The activity database also maintains a table of event attributes which are needed for event analysis, represented by $ATTR_{ij,k}$. e.g.: For checking account event the attributes could be: *Time of login; Number of attempts; Location; IP address; Phone number; etc.*

Symptoms database

The symptom is defined as an evidence of security attack or damage. The symptoms database stores the set of symptoms to be watched during the time of particular event analysis, which are represented by $S_{ij,k}$. Each symptom is associated with a value, which serves as weight to be given for that particular symptom aroused during event analysis. e.g.: For placing purchase order event, the symptoms could be: *Suspicious transaction time; Suspicious transaction amount; Suspicious frequency; Suspicious product details; etc.*

Customer behavior profile

In the proposed system the customer profile is built using transactions history of a customer in a given time frame. The profile essentially deals with the purchasing behavior of the customer. The Customer class has been worked out on the basis of average transaction value and frequency of changing vendors. The preferences entirely depends on the various probabilities computed over previous transaction data.

Vendor behavior profile

The vendor behavior profile has been constructed using the business history of the vendor. The vendor profile is used to establish the credibility of the vendor, by accumulating the statistics of the business operations conducted. The vendor class is identified based on the range of goods the vendor sells, the discount strategy, after sales service rank is computed using shipping time, replacement commitment, complaint handling, etc.

4. The IFDS

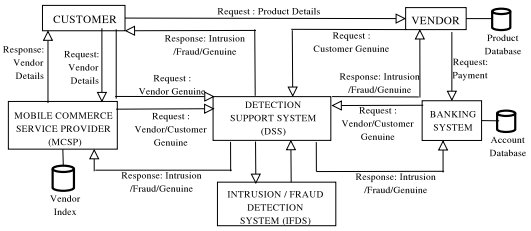

Figure 1. Mobile commerce architecture with IFDS.

The proposed AES model detects all the attempts happens in customer and vendor accounts due to subscription fraud and device theft risks in mobile commerce environment. We have made use of the behavior profiles of customer and vendor in order to detect the symptoms of intrusions and frauds, along with the various databases discussed in the previous section. All the databases have been designed keeping the mobile commerce services in mind. We assume the existence of cellular and wireless communication infrastructure for mobile device operations and the industry standard cryptographic techniques are in place for secured communication between various entities. All the channels are of type secured and the entities like MCSP, DSS and Banks are possessing the digital certificates issued by Trusted Third Party in order to establish mutual authentication. The system aspect is shown in Fig. 1, where all the entities in mobile e-commerce environment interacts with IFDS for the purpose of detecting intrusion and fraud attempts happens in various transactions conducted. The AES model is shown in Fig. 2, the activity monitor module is responsible for identifying events and attributes for the activity received from DSS. Next, events analyzer will use these data to detect suspicion factor for the event under execution. Finally, a symptom monitor module provides a set of symptoms to be observed during event analysis.

Activity Monitor

The function of this module is to receive the request from DSS for checking the mobile commerce activity whether it is suspicious or not. The activity monitor is responsible for maintaining activity database for location based mobile commerce services and it captures the attributes for the various events initiated during the activity execution. It passes the event and attributes to Events Analyzer for pronouncement of intrusion or fraud. The Algorithm 1 discusses the functions of the activity monitoring process.

Events Analyzer

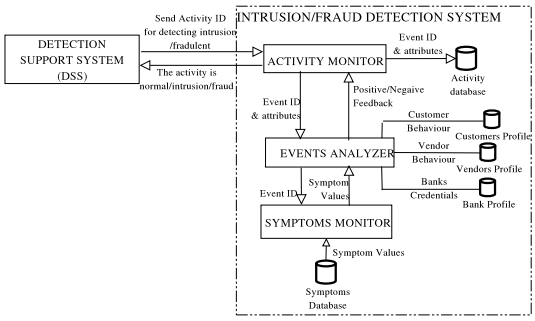

Figure 2. AES model

Algorithm 1 Algorithm for Activity Monitor module

1: Begin
2: Initialize the Certainty Factor(CF) for the new activity A_i.
3: **repeat**
4: Accept the activity ID A_i.
5: Extract concerned eventID(s) from activity database. Let $E_{ij} = E_{i1}, E_{i2}, \ldots, E_{in}$
6: **for** $j = 1$ to n **do**
7: Capture the values for attributes of event E_{ij}, say $ATTR_{ij}$
8: Pass E_{ij} and $ATTR_{ij}$ to Events Analyzer.
9: Wait for the feedback from Events Analyzer.
10: **if** Feedback is Negative **then**
11: The activity is suspected and pass the alert to DSS.
12: **end if**
13: **end for**
14: The activity is not suspected and pass the feedback to DSS.
15: **until** No more activities
16: End

This module accepts an event and its concerned attributes from the Activity Monitor and performs event analysis in coordination with Symptoms Monitor. The Algorithm 2 describes the Events Analyzer functioning. This module uses the profile databases of customer and vendor, which includes service usage patterns, service providing patterns and network usage patterns during event analysis. The Events Analyzer identifies the deviation between current event attributes and profiled attributes using suitable check conditions, which are nothing but carefully laid out rules for detecting suspicious events. It computes the Suspicion Factors for all the symptoms for that event and generates the Cumulative Suspicion Factor(CSF) for the whole event. Further the suitable threshold is applied to determine the chances of intrusions or frauds.

Symptoms Monitor

The Symptoms monitor maintains symptoms database, the module returns the symptoms set $S_{ij,k}$ and weight set $W_{ij,k}$ to Events Analyzer. The symptoms are essentially the quantities to be observed while detecting the suspicious activities and weights are the allotted priorities to various

Algorithm 2 Algorithm for Events Analyzer module

1: Begin
2: Initialize the Cumulative Suspicion Factor(CSF) for the new activity A_i.
3: **repeat**
4: Accept the event E_{ij} and $ATTR_{ij}$ from the Activity Monitor.
5: Initialize the Suspicion Factor(SF) for E_{ij}.
6: Obtain the intrusion/fraud symptoms for E_{ij} from Symptom Monitor, say S_{ij}.
7: **repeat**
8: Select the symptom s from S_{ij} and corresponding weightage w from W_{ij}.
9: Execute Check Condition C or combination of Check Conditions over $ATTR_{ij}$ and profiled attributes, to obtain the deviation.
10: Check the deviation is suspicious based on s.
11: Compute the SF for the event E_{ij} using w of the symptom s.
12: $CSF = CSF + SF$.
13: **until** No more symptoms in S_{ij}.
14: Select Appropriate $Threshold$.
15: **if** $CSF >= Threshold$ **then**
16: Pass Negative feedback to Activity Monitor.
17: **else**
18: Update the $Threshold$ if necessary.
19: Pass Positive feedback to Activity Monitor.
20: **end if**
21: **until** No more events
22: End

Algorithm 3 Algorithm for Symptoms Monitor module

1: Begin
2: **repeat**
3: Get the event E_{ij} from the Events Analyzer.
4: Retrieve symptoms related to E_{ij} from symptoms database and corresponding weights W_{ij}.
5: Return symptoms set S_{ij} and W_{ij} to Events Analyzer.
6: **until** No more events
7: End

symptoms. Algorithm 3 gives the Symptoms Monitor functioning.

5. Simulation

We have established the wireless testbed as shown in Fig. 3 to test the working of our proposed system. Various mobile devices used in testbed includes Samsung X10 Laptop with 802.11b/g WiFi connectivity, HP iPAQ rx3715 PDA with Bluetooth, IEEE 802.11b and IrDA connectivity, HP iPAQ h6365 PDA with IEEE 802.11b, Bluetooth and GSM/GPRS connectivity and CDMA enabled mobile phone. The Cisco Acess Point AiroNet 1200 series gateway is used for wireless networks and one of the CDMA/GSM

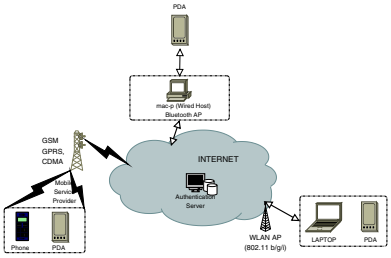

Figure 3. Mobile commerce simulation environment.

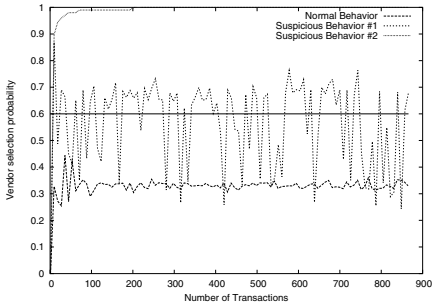

Figure 4. Vendor selection behavior

mobile service is used for cellular networks.

The mobile commerce purchasing scenario is implemented over the established wireless testbed for detecting fraud. The customers are categorized into three classes namely low-profile, medium profile and high-profile based on the product selection behavior. Based on this classification the mean of transaction amount and maximum limit of transaction amount for each class are worked out. Each class of customers is further categorized into three classes namely Class-1, Class-2 and Class-3 based on the vendor selection behavior. Class-1 customers quite frequently changes the vendor, Class-2 customers changes vendor with moderate frequency and Class-3 customers very rarely changes the vendors. The class-wise probability thresholds for doing business with particular vendor are fixed based on this classification. We have conducted various experiments using the simulation environment, to analyse the performance of the proposed system.

5.1 Results and discussion

A fraudulent transaction requires the fraudster to be in possession of the customer signature, such as PIN or password, and also to be able to send the response message to the payment provider. In some occasions the fraudster behaves as if he/she is a customer. This kind of fraud is known as subscription fraud, where the attacker will take over the customer accounts and perform transactions. Figure 4, denotes three behaviors of the class-2 customer with respect to selecting vendor to perform purchase. The probability threshold was established class-wise, here it is 0.6 for class-2 customer. Any considerable deviation from the threshold generates high suspicion factors. The normal behavior of the customer shows the probability of selection of vendor is well within threshold 0.6. Where as the suspicious behavior raises the vendor probability to more than threshold because the fraudster may purchase repeatedly from the same vendor. The suspicion factor for vendor selection is computed using probability of vendor selection, and probability of buying from a vendor for a particular customer class.

The Figure 5, represents three behaviors of the class-2 customer with respect to transaction amount. The normal behavior shows that the difference in means are almost constant. The intruder behavior shows that there is more fluctuations in the difference of mean, this is due to desultory selection of items for purchase by fraudster. The suspicion factor on transaction amount is computed using mean of transaction amount fixed for a particular customer class, and ceiling amount allowed for transaction for a particular customer class.

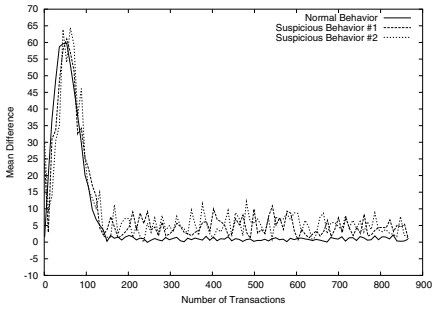

Figure 5. Purchasing value behavior

The Figure 6, represents three behaviors of the class-2 customer with respect to frequency of purchase. It has been analyzed using the time difference between two successive transactions. Commonly the normal behavior has time difference between the transactions which is approximately equal to the average time difference, whereas the suspicious behaviors exhibits the hurry in purchase with decreased time difference between transactions. The suspicion factor on frequency is computed using the time at which current transaction is happening, and the time at which last transaction was happened.

The Figure 7, represents three behaviors of the class-2 customer with respect to purchase in various week days. It has been analyzed using the probability of purchase in various week days. We can observe from the result that suspicious behavior probabilities varies considerably from the normal behavior probabilities, since the fraudster choice of purchasing days is bizarre in comparison with genuine customer. The suspicion factor on day of purchase is computed

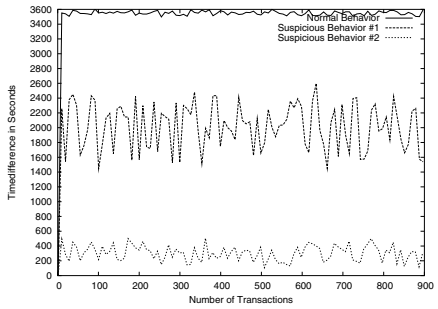

Figure 6. Frequency of purchase behavior

as using probability of purchase generated for a day , and the profiled value of probability of purchase.

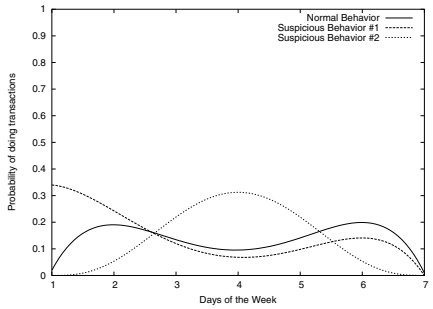

Figure 7. Purchasing in various week days behavior

The Figure 8, represents three behaviors of the class-2 customer with respect to purchase in various hours of a day. It has been analyzed using the probability of purchase in various hours in a week day. We can observe from the result that suspicious behavior probabilities varies considerably from the normal behavior probabilities, since there will be a time difference between one geographical region to another in case of fraud happen from another demography or the fraudster may choose his own convenient times for purchase which may vary from the normal. The suspicion factor on time of purchase is computed using the probability of purchase generated for hour during the time frame considered for analysis, and the profiled value of probability of purchase for hour from the history of transactions.

The Figure 9, shows the suspicion factors generated by various transactions by class-2 customer. The suspicion factor is the accumulation of various suspicion values generated by different symptoms of fraud. The threshold 0.5 marks the maximum suspicion allowed, after which the transactions are considered as fraud and further investigations will takes place on the usage of customer account.

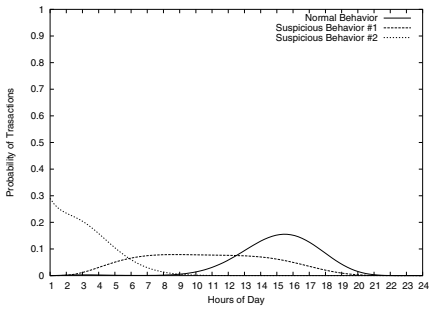

Figure 8. Purchasing in various hours of a day behavior

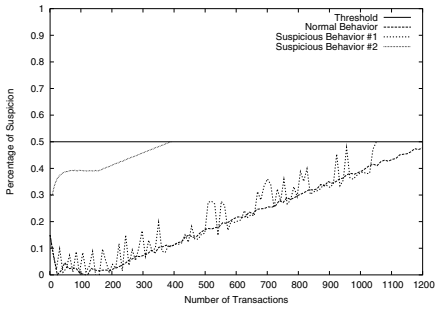

Figure 9. Cumulative suspicion factor

6. Conclusion

The proposed scheme identifies the intrusions/frauds happening in customer accounts and vendor accounts by identifying the various suspicious symptoms in business transactions. The system emphasize on-line analysis of transactions instead of offline analysis. The use of weighed symptoms will make the identification process faster compared to other techniques.

References

[1] D. P. Cahill, M. H. Lambert and D. X. Sun. *Detecting fraud in real world*. chapter in Handbook of Massive Datasets, 2000.

[2] D. Guerin. Fraud in electronic payments. Technical report.

[3] S. Kumar. Classification and detection of computer intrusions a ph.d. thesis. Technical report, 1995.

[4] W. Lee and K. W. Mok. Adaptive intrusion detection: a data mining approach. *Artificial Intelligence Review*, 14, 2000.

[5] S. Nambiar and C.-T. Lu. *M-Payment Solutions and M-Commerce Fraud Management*. Chapter IX from the book Advances in Security and Payment Methods for Mobile Commerce.

[6] J. B. S. Freeman, A. Bivens and B. Szymanski. Host-based intrusion detection using user signatures. In *Proceedings of Graduate Research Conference*, 2002.

[7] U. Varshney and R. Vetter. A framework for the emerging mobile commerce applications. In *Proceedings of HICSS '01*, 2001.