International Journal of Security and its Applications
Vol. 2, No. 4, October, 2008

Performance Analysis of an Authentication Scheme for Personalized Mobile Multimedia applications: A Cognitive Agents based Approach

B. Sathish Babu and Pallapa Venkataram
Protocol Engineering Technology Unit,
Electrical Communication Engineering,
Indian Institute of Science, Bangalore, India.
E-mail:{bsb,pallapa}@ece.iisc.ernet.in

Abstract

Personalized Multimedia (PMM) services are the emerging area in multimedia technology. A PMM service is a multimedia service provided according to the users personal profile which typically includes individual preferences, keeping the technical constraints of mobile device in use and the operating environment. We have proposed in [2], a transaction-based authentication scheme for PMM applications using cognitive agents. The proposed approach dynamically deploys authentication challenges based on mobile transaction sensitivity and users transaction time behaviors. This paper provides performance analysis of the authentication scheme in terms of authentication delay and cost. The performance analysis shows that, there is a considerable reduction in security cost compared to regular session based authentication schemes. By combining transaction based authentication with behavior analysis authentication attacks can be effectively identified.

1. Introduction

Personalized multimedia(PMM) is a service provided according to the users personal profile which typically includes individual preferences, keeping the technical constraints of a mobile device in use and the operating environment. Since mobile services are typically accessed from different types of mobile devices, device independence and personalization play an important role in the PMM services. Any system which provide PMM services has facility where an user can able to specify

[0]Part of the paper is presented in FGCN 2007.

their own preferences for driving the creation, transmission and consumption of multimedia content.

Some of the PMM services transactions are as follows: Sending a service request from a mobile device to record program broadcast on some television channel. Remotely controlling the accessories using mobile devices, and sanctioning authorization to use accessories. Providing personalized location based tourist information based on the established personal profile, which includes users needs interests, and preferences. Picking up the reserved car from parking lot on arriving to aerodrome just by identification and authorization via mobile device, and so on.

"Customization" is a mantra of any PMM service implementations. The customization is application dependent rather generic. In Cellware [10], customization is done using registered events multimedia content, and user preferences. The generic tourist guides in PMM applications [3] [8], are proposed for applying to any city and any place. The iMobile [4], is a proxy-based mobile service platform designed to provide PMM services, it renders information based on the user and device profiles. The policy driven PMM service proposed in [6], describe a set of co-operative agents distributed over different sites that work together to provide personalized services for mobile users over the Internet. The UPMSM model [12], proposes a ubiquitous personalized multimedia service model based on finite state machines.

Authentication in context of the PMM service is a process to identify a mobile user(customer), in order to authorize him/her to use the specified PMM service. The primary aim of any authentication protocols is "verifying the linkage between an identifier(usually claimed by the individual, but sometimes observed) and the individual." An important issue of authentication in the PMM service platform is, "how does it determines who the mobile user is, if requests are allowed to come in from various communication channels and devices." There is a requirement of high security standards in personalization: no part of a user profile should be compromised, eavesdropped, adulterated or maliciously modified during service execution [11].

Device/terminal based authentication protocol is one of the common type of authentication practiced by mobile based application service providers. Here, it is essential to register the device in advance to use the service. Even though this authentication mechanism looks stringent, it does not able to detect service misuse from compromised mobile devices. It also indirectly limit the users freedom of changing the device at his/her will, which is very common in a mobile environment.

In our scheme, we use intellective approach for the PMM user authentication using a type of intelligent agents called cognitive agents (CAs). These are the agents with high reasoning capability to solve complex real time problems which have high degree of dynamism. Since the service usage pattern and default pro-

files of the clients will play a crucial rule in the personalization of mobile services [11], the dynamism we are incorporating for proposing transaction-based authentication is service and transaction time behaviors of the PMM users. In mobile environment, the user behavior is highly volatile it changes with service, device, network, distance, time, location, cost, etc. Therefore a signature/anomaly detection schemes used in wired networks can not be efficient in mobile systems. A rational approach towards identifying the correct principal can be established by using these type of agents, which is very much essential in mobile environment where real time classification of attacker from a genuine user is a challenge.

The proposed PMM services transaction-based authentication scheme(PMM-TBAS) use two types of cognitive agents: the *mobile cognitive agent (MCA)* and the *static cognitive agent (SCA)*, which are secured with respect to their construction and inter communication. The total authentication scheme is distributed into two logical components: the MCA based component and the SCA based component. The SCA creates MCA and sends to respective user mobile device, when a user need to be authenticated for the PMM services. The MCA generates beliefs over user service transactions by observing various behaviors, and these beliefs are sent to SCA for analysis. The SCA dynamically generates authentication requirements based on the sensitivity of the service transactions and the changing beliefs on users. The application-based challenge/response protocol has been incorporated to counteract some common misuse of services by attackers.

The rest of the paper is organized as follows, section 2 provides some related works on the PMM services authentication, section 3 gives the definitions of terminologies used in the paper, section 4 discusses the functioning of proposed authentication system, section 5 illustrates analytical modeling of the belief analysis, authentication delays and costs, section 6 provides simulation results, and finally section 7 draws conclusions.

2. Related works

In [6], H. Harroud et al, propose use of session keys generated by the user authentication procedure given in [5] for policy-driven PMM services. To authenticate a client, an authentication agent is activated by receiving coordinator manager(CM). The agent proposes an authentication and key exchange protocol and sends it back to visiting CM. The visiting CM then decides whether or not to activate the visiting site authentication agent according to the local site security policy.

Y. Chen et al, in [4], consider each service request is sent to a command dispatcher hosted on the proxy. The dispatcher authenticates the users validates the command, and decides which infolets(which are responsible for obtaining informa-

tion from various data sources or content providers) or applets (which implements the application logic by postprocessing information obtained by the various infolets) to invoke to service the request.

In the Simplicity Project: Personalized and simplified communication spaces for mobile users [9], R. Seidl et al, provides the authentication and payment functionality based on SD-login. the Simplicity Device(SD)-login which may be a plug-in physical device (e.g., Java card, Java ring, enhanced SIM card, USB pen, etc.) or a functional entity (e.g., a software agent) that stores user preferences.

All the above mentioned authentication procedure for PMM service are static in nature. They provide common scheme of authentication irrespective of the sensitivity of the service going on. These works didn't explored possibility of real time analysis of service transactions, in order to propose the required level of authentication dynamically. Therefore it is difficult to distinguish between genuine user and an attacker based on only authentication identifiers. A transaction-based authentication scheme is one of the solution proposed in this direction, which will enable a strong authentication at a transaction level of the PMM service.

3. Definitions

In this section we provide definitions for terminologies used in the paper.

Behaviors: The behaviors refer to the actions or reactions of a PMM user while using the PMM services. The behaviors are derived based on the transaction data or the data gathered from physical actions and attitudes of the user. Some of the behaviors of the user in touring system are: *visiting only historically important places, always staying in medium range hotels, using railways in journey, preferring continental food, changes plans frequently, always moves alone, and so on.*

Observations: An observation is the summarization of various behaviors exhibited by the user during service execution. Based on the behaviors listed above in a touring system, some of the observations are derived over: *cost-consciousness, food-specificness, journey-interests, place-liked, and so on*.

Beliefs: Primarily the "beliefs represent information about the world or an entity, perceptions received from an external world and execution of events update the beliefs ". In a touring system example, some of the beliefs on a customer are: *low-profile visitor, high-profile visitor, philosophical, pilgrimage, archaeologist, and so on.*

PMM authentication database: This database resides at the SCA and, is used to perform required authentication based on the sensitivity level of the transactions. The database includes various authentication related information for each transaction level. The database record includes *Authentication data set for each transac-*

tion level, account information, and behavior/physical biometric information for critical transactions.

PMM beliefs database: The beliefs database at the SCA stores the probability values for the various beliefs w.r.t. a PMM service user. The beliefs have been represented using the probabilistic values. The contents from the belief database is used to estimate the belief deviation during transactions. The frequency at which the beliefs database is updated is application dependent, since some applications like shopping witness more frequent changes in behaviors compared to applications like touring, where the behaviors remains consistent over a long period of time. The belief database has been constructed using history of transactions.

Service log: The service provider maintains the detailed log of all the transactions conducted by the mobile users. The structure of the database is service dependent, and the contents can be used to construct transaction based challenges. For example, a challenge question like *Which is your favorite touring spot?* can be created by using users transaction log in a touring system application.

Observations storage: This is a temporary storage available at the MCA for storing generated observations during the transactions session. The content of this storage is used for belief generation and analysis.

4. The PMM-TBAS using CAs

The information sensitivity and length of secrets are the key factors in proposing security levels for information systems. As we observe, not all the mobile transactions have same classified information. Therefore, we argue that the nature of transactions should be involved to classify the security levels, there by authentication actions could be applied categorically. We propose in [1], classification of mobile transactions into four security classes (Level-0 to Level-3) based on the degree of severity of information that they are handling, and the magnitude of risk involved due to misappropriation of transactions. The degree of severity can be gathered from the policies laid out by service providers/organizations.

As we discussed earlier, the PMM-TBAS constitutes two major parts: SCA-part and MCA-part. The working of the total authentication scheme requires deployment of SCA either at home agent(HA) in home network and/or at the foreign agent(FA) in foreign network. The PMM-TBAS plays a complementary role to already established security infrastructure which include PKI portals and Certifying Authorities (CAs), and it may be incorporated as separate modules in security servers in a network or may be incorporated into existing security infrastructure.

The SCA component essentially performs three functions; 1. Transaction based authentication; 2. Beliefs analysis; and 3. Challenge/response. An instance of a

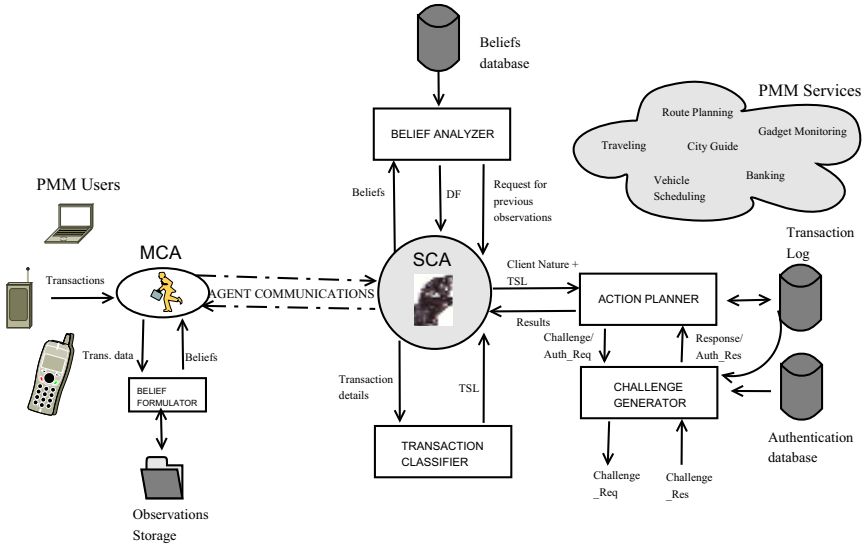


Figure 1: The PMM-TBAS architecture.

mobile cognitive agent(MCA) is created by the SCA and migrated it to a mobile node during registration, which is used to formulate beliefs over users transaction time behaviors. The SCA finds sensitivity of transaction to be executed, and determines the authentication level needed for that transaction. The belief analyzer operated by SCA is used to determine at what factor the current beliefs over a mobile user are deviating from established beliefs. The challenge/response module is used to generate appropriate authentication challenges based on requests received from transactions authenticator and beliefs analyzer.

When the customer at home network/foreign network wish to perform transactions with respect to some service, he/she contacts the agent situated in that particular network for registration. We assume here, the customer registration with the network will follow some standard registration protocol available, e.g. Mobile IP(MIP). After successful registration the PMM-TBAS at the corresponding agent will migrate an instance of MCA to the mobile device of the customer. In this section we explain the roles of the MCA and the SCA in the proposed system, and also we provide brief functioning of the PMM-TBAS components. The architecture of the PMM-TBAS system is shown in Fig. 1.

MCA

When a PMM service request is initiated by the user, the MCA migrates to a client along with *belief formulator* logic. The MCA communicates the gener-

Algorithm 1 Working of MCA

```
1: Begin
2: Input: Transactions T submitted by customer.
3: Output: Beliefs set B and T.
4: Observations Storage ⇐ NULL
5: while Not end of session do
6:    Accept T.
7:    B ⇐ BeliefFormulator(T).
8:    Send B and T to SCA.
9:    if Any request for observations from SCA then
10:      Select observations from Observations Storage.
11:      Send selected observations to SCA.
12:   end if
13:   Periodically refresh Observations Storage.
14: end while
15: End
```

ated beliefs along with parameter values to SCA on every customer. It logs in all new observations into *observation storage*, stores them for fixed period of time, and refreshes the storage periodically. Based on the request from SCA, the MCA provides the previous observations stored. The functioning of MCA is given in Algorithm 1.

Belief Formulator

The belief formulator is a component of MCA which collects various temporal and symptomatic behavior parameters from the client transactions and its context. It computes transaction time behaviors of the client and generates the observations. The beliefs are deduced based on the new and available observations over a customer. For example, if the transaction time behaviors of the PMM touring system customer has observations such as:*unplanned staying, random selection of visiting places, frequent changes in visit plans, etc.,* the agent produces the belief over a customer as *fickle-minded visitor.* The belief formula which is used to represent individual belief is given by: $(p - belief, t_1, \ldots, t_n)$. Where *p-belief* is the predicate used to claim a value for a particular belief and t_1 to t_n are terms, which are literals and variables used to represent various observations on which the belief is reasoned. The given belief representation is compatible with cognitive agents created using agent factory system (AFS) [7], and the working of *belief formulator* is given in Algorithm 2.

SCA

The SCA co-ordinates with all the components of the system at the security

Algorithm 2 Algorithm for Belief Formulator

1: Begin
2: **Input:** Transactions T.
3: **Output:** Beliefs set B.
4: Begin
5: Initialize belief data structure of agent.
6: **for** Each transaction T **do**
7: Let V= $\{v_1, v_2, \ldots, v_k\}$ is the set of values collected by agent for various temporal and symptomatic behavior parameters from transaction T.
8: $\forall\ b_i \in$ belief data structure, select those beliefs which are fired from observations generated using V.
9: Add all selected beliefs into B.
10: **end for**
11: Return B.
12: End

server, it is responsible for migrating MCAs to various mobile devices and carrying out communications with MCAs. Upon receiving the beliefs and parameter details from MCAs, the SCA submits them to *belief analyzer* for the purpose of finding the deviation in new beliefs and the established beliefs of the customer. Based on the value of total deviation factor (TDF), and thresholds for normal and suspicious behaviors, the SCA produces one of the following three types of opinions on the PMM user-nature: *NORMAL-USER, SUSPICIOUS-USER, ABNORMAL-USER*. The results are passed onto *action planner* for suitable authentication actions. The SCA also fetches the observations from MCA on request from *belief analyzer*. The functioning of SCA is given in Algorithm 3.

Belief Analyzer

It accepts newly generated beliefs on the PMM user from the SCA, and correlates them with established beliefs of the PMM user from beliefs database in order to identify the deviation. The deviation function could be designed based on type of parameters, and service under consideration. The deviation function must require to satisfy distance property, where increased distance between two corresponding behavior values should produce higher deviations, and vice versa. For example, in a PMM touring system, higher deviations are generated when the choice of visiting spots from pilgrim type of customer changes to discotheques and casinos. The Algorithm 4 is used by *Belief Analyzer.*

Transaction Classifier

Transaction classifier accepts transaction details submitted by the PMM user from the SCA and find the transaction sensitivity level (TSL). The TSL is gener-

Algorithm 3 Working of SCA

1: Begin
2: Initialize TDF to zero.
3: **while** Not end of user session **do**
4: Accept B & T from MCA.
5: $DF \Leftarrow$ *BeliefAnalyzer*(B).
6: $TSL \Leftarrow$ *TransactionClassifier*(T).
7: **if** There is any request from *Belief Analyzer* for observations **then**
8: Fetch them from MCA.
9: **end if**
10: **if** There is any request from *Belief Analyzer* for new beliefs **then**
11: Fetch the beliefs from SCA of customer's home network.
12: **end if**
13: Pass transaction details to *Transaction Classifier*.
14: Add DF to TDF.
15: **if** TDF $< Th_{normal}$ **then**
16: **User-nature** $\Leftarrow$ *NORMAL-USER*.
17: **else if** TDF $\geq Th_{normal}$ and TDF $< Th_{suspicious}$ **then**
18: **User-nature** $\Leftarrow$ *SUSPICIOUS-USER*.
19: Generates additional beliefs (if required).
20: **else if** TDF $\geq Th_{suspicious}$ **then**
21: **User-nature** $\Leftarrow$ *ABNORMAL-USER*.
22: **end if**
23: **Authentication-result** $\Leftarrow$ *ActionPlanner*(User-nature, TSL).
24: **if Authentication-result** is Failure **then**
25: Disconnect the client session.
26: Deallocate MCA from mobile node.
27: **else**
28: TDF = TDF - DF.
29: **end if**
30: **end while**
31: End

ated by analyzing various transaction parameters, like, *type of operation; time of operation; type of data; sensitivity of data; volume of data; device used, location of operation, velocity of mobility, etc.* This analysis produces the TSL ranging from level 0 to 3. The sample logic for *transaction classifier* is given in Algorithm 5.

Action Planner

Based on the values of TSL and opinions on the PMM user, the *action planner*

Algorithm 4 Algorithm for Belief Analyzer

1: Begin
2: Accept B from SCA.
3: $DF \Leftarrow 0$.
4: $B^{new} \Leftarrow B$.
5: Retrieve the established belief on customer from beliefs database; say, $B^{established}$.
6: **if** The $B^{established}$ is not present **then**
7: Send request to SCA to fetch from home network.
8: **end if**
9: **if** $|B^{established}, B^{new}| \geqslant Threshold_{deviation}$ **then**
10: **if** Observations are required for belief analysis **then**
11: Send request to SCA to fetch from MCA.
12: **end if**
13: **for all** ${bh_i}^{new} \in B^{new}$ **do**
14: Compute deviation factor for each behavior ${bh_i}^{new}$ w.r.t. ${bh_i}^{established}$; let, Dev_{bh_i}.
15: $DF \Leftarrow DF + Dev_{bh_i}$.
16: **end for**
17: **end if**
18: Return DF.
19: End

perform the following. All the TSL(=0) transactions are executed without any authentication by the system. If TSL(>0) and transactions are appearing for the first time, it instructs the *Challenge generator* to perform initial authentication for that transactions level. Otherwise, the action planner decides its future actions based on the value of user nature.

Challenge Generator

This module is responsible for generating authentication challenges and attacks counteracting challenges during transaction execution. In order to safeguard challenge system from phishing attacks, the challenges are encrypted using the security algorithms of the corresponding transactions sensitivity levels. These security algorithms are known to agents. The MCA at PMM user side, decrypts challenge, obtains response from PMM user and send the encrypted response to challenge/response module. Some of the example of challenges in a PMM touring system are: *Which year you have last visited this place?; Which is your favorite airways?, etc.* The Algorithm 7, shows the working of challenge generator.

Algorithm 5 Logic for Transaction Classifier

```
Begin
Accept transaction details T from SCA.
Let OP is the operation requested by transaction T.
if OP is "Using PMM service" then
    Let TYPE is the type of PMM service to be used.
    if TYPE is Free-Service then
        TSL = 0.
    else if TYPE is Personal-Service then
        TSL=1
    else if TYPE is Confidential-Service then
        TSL=2
        /* More analysis on type of service – follows*/
    end if
else
    if OP is "Authorizing PMM service" then
        Let TYPE is the type of PMM service to be authorized.
        if TYPE is No-risk-Service then
            TSL = 0.
        else if TYPE is Less-risk-Service then
            TSL=1
        else if TYPE is Medium-risk-Service then
            TSL=2
            /* More analysis on type of authorization – follows*/
        end if
    end if
end if
Pass TSL to SCA.
End
```

5. Analytical Modeling

In this section we have provided the analytical models for the proposed system. The belief analysis model is used during finding out belief deviations, the models for computing authentication delay at different sensitivity levels of transactions and corresponding security costs are provided.

Belief Analysis

The belief generation of the PMM-TBAS is organized hierarchically as shown in the Fig. 2. When the transactions are initiated by the customer new values

Algorithm 6 Algorithm for Action planner

```
1: Begin
2: for Each each transaction T do
3:    Accept TSL and User-nature from SCA.
4:    if TSL is 0 then
5:       Pass Authentication success message to SCA.
6:       Execute transaction T.
7:    else if TSL is not encountered before then
8:       Instruct Challenge Generator to perform initial authentication data of that
         TSL.
9:    else if User-nature is NORMAL then
10:      Pass Authentication success message to SCA.
11:      Execute transaction T.
12:   else if User-nature is SUSPICIOUS then
13:      Instruct Challenge Generator to get the next authentication data of that
         TSL.
14:   else if User-nature is ABNORMAL then
15:      Instruct Challenge Generator to create transaction-based challenges.
16:   end if
17:   if The response from Challenge Generator is "Success" then
18:      Pass Authentication success message to SCA.
19:      Execute transaction T.
20:   else
21:      Roll-back transactions of that session.
22:      Pass Authentication failure message to SCA.
23:   end if
24: end for
25: End
```

for behavior parameters are captured. Based on these values, the MCA computes probabilities of occurrence of various behaviors, observations and beliefs for the current session(which are suffixed by new). Let, the probability P_{Bh_i} of generating the behavior Bh_i is computed using the behavior parameters set BP_i. The required number of behavior parameters varies from one behavior to another. It is also possible that, the same behavior parameters may produce different behaviors based on the value they acquired. For example the behavior parameters like: *time-of-login, location-of-login, device-used-for-login, number-of-login-failure-attempts, and so on*, may produce the behaviors such as "stranger entering user account" and "the regular user behaving abnormally". So, intuitively we can say the behavior

Algorithm 7 Algorithm for Challenge Generator

```
Begin
if Transaction appearing first time and TSL > 1 then
    Create encrypted challenge to perform initial authentication of TSL.
else if User-nature is SUSPICIOUS then
    Create encrypted challenge for that TSL over Next data from authentication
    data set.
else if User-nature is ABNORMAL then
    Create encrypted challenge for that TSL over Transaction Log.
end if
Decrypt and validate the response obtained from the user.
if Response is correct then
    Send "Success" to Action planner.
else
    Send "Failure" to Action planner.
end if
End
```

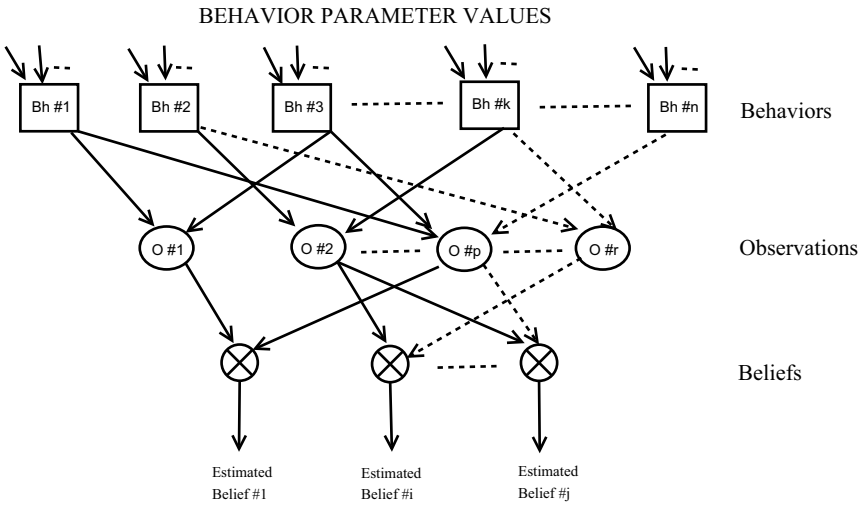


Figure 2: Belief generation model

sets are either joint or disjoint.

$$P_{Bh_i}{}^{new} = \frac{\sum_{k \in BP_i} W_{bh_k} * V_{bh_k}}{\sum_{k \in BP_i} Max_{bh_k}} \qquad : \sum_{k \in BP_i} W_{bh_k} = 1 \qquad (1)$$

Where W_{bh_k}, V_{bh_k}, and Max_{bh_k} are the weight, current value, and the maximum possible value of the behavior parameter bh_k respectively.
The observation probability P_{Ob_i} is computed using the union of occurrence of defined set of behaviors which leads to that observation. Since the behaviors are joint or disjoint, we used union instead of summation. Let BH_{Ob_i} is the set of behaviors considered for observation Ob_i.

$$P_{Ob_i}{}^{new} = P(Bh_a{}^{new} \cup Bh_c{}^{new} \cup Bh_k{}^{new} \cup \cdots \cup Bh_m{}^{new}) \tag{2}$$

Where $Bh_a{}^{new}, Bh_c{}^{new}, Bh_k{}^{new}, \ldots, Bh_m{}^{new} \in BH_{Ob_i}$.

The probability of occurrence of a belief P_{Bl_i} is the union of those observations which will generate the particular belief. The union intuitively represents the observations may be joint or disjoint. Let O_{Bl_i} is the observations set for belief Bl_i.

$$P_{Bl_i}{}^{new} = P(Ob_c{}^{new} \cup Ob_f{}^{new} \cup Ob_l{}^{new} \cup \cdots \cup Ob_n{}^{new}) \tag{3}$$

Where $Ob_c{}^{new}, Ob_f{}^{new}, Ob_l{}^{new}, \ldots, Ob_n{}^{new} \in O_{Bl_i}$.

The SCA calculates the deviation factor between the probability values of beliefs received from MCA, i.e., $P_{Bl}{}^{new}$, with the corresponding established probability values of beliefs in beliefs database, i.e., $P_{Bl}{}^{old}$.

$$D(Bl^{new}, Bl^{old}) = |P_{Bl}{}^{new}, P_{Bl}{}^{old}| \tag{4}$$

Exponentially moving averages are used to accumulate deviation factors of beliefs generated during various transaction instances. The weights for each transaction decreases exponentially, giving much more importance to current deviation while still not discarding older deviations entirely. The smoothing factor α is given by.

$$\alpha = \frac{2}{NumberofTransactions + 1} \tag{5}$$

The cumulative deviation factor for beliefs at time t is given by,

$$CDF^t{}_{Bl} = \alpha * D(Bl^{new}, Bl^{old}) + (1 - \alpha) * CDF^{t-1}{}_{Bl} \tag{6}$$

Thresholds have been established in order to take security actions, namely $Th_{suspicious}$ and $Th_{abnormal}$. The CDF within $Th_{suspicious}$ refers to transactions are normal. If the CDF is between $Th_{suspicious}$ and $Th_{abnormal}$, then the transactions are suspicious. When the CDF exceeds $Th_{abnormal}$ then the transactions are bizarre. Values for thresholds are computed using statistical deviation $SDev$ over the set of newly generated beliefs Bl^{new}, the weightage W_{Bl} assigned to various beliefs

based on history, and the step function γ provides distance between $Th_{suspicious}$ and $Th_{abnormal}$.

$$SDev_{Bl_i} = \sum_{i \in Bl^{new}} \sum_{j \in Bl^{new}} P_{Bl_i} * D(Bl_i, Bl_j) \tag{7}$$

$$Th_{suspicious} = \sum_{i \in Bl^{new}} W_{Bl_i} * SDev_{Bl_i} \quad : \sum_{i \in Bl^{new}} W_{Bl_i} = 1 \tag{8}$$

$$Th_{abnormal} = Th_{suspicious} + \gamma \tag{9}$$

$$\gamma = \frac{\sum_i^n ({Th_{suspicious}}^i - \mu)^2}{n} \tag{10}$$

Where μ is the mean of $Th_{suspicious}$ computed so far, and n is the number of times thresholds are computed.

Average authentication delay

The delay in authentication of a transaction is defined as time taken for a customer to receive the authentication reply for the request. The average authentication delay T_{avg}, is defined as the sum of an authentication delay over a number and type of transactions in a unit time.

$$T_{avg} = \sum_{l=0}^{3} \lambda_l {T_l}^i \tag{11}$$

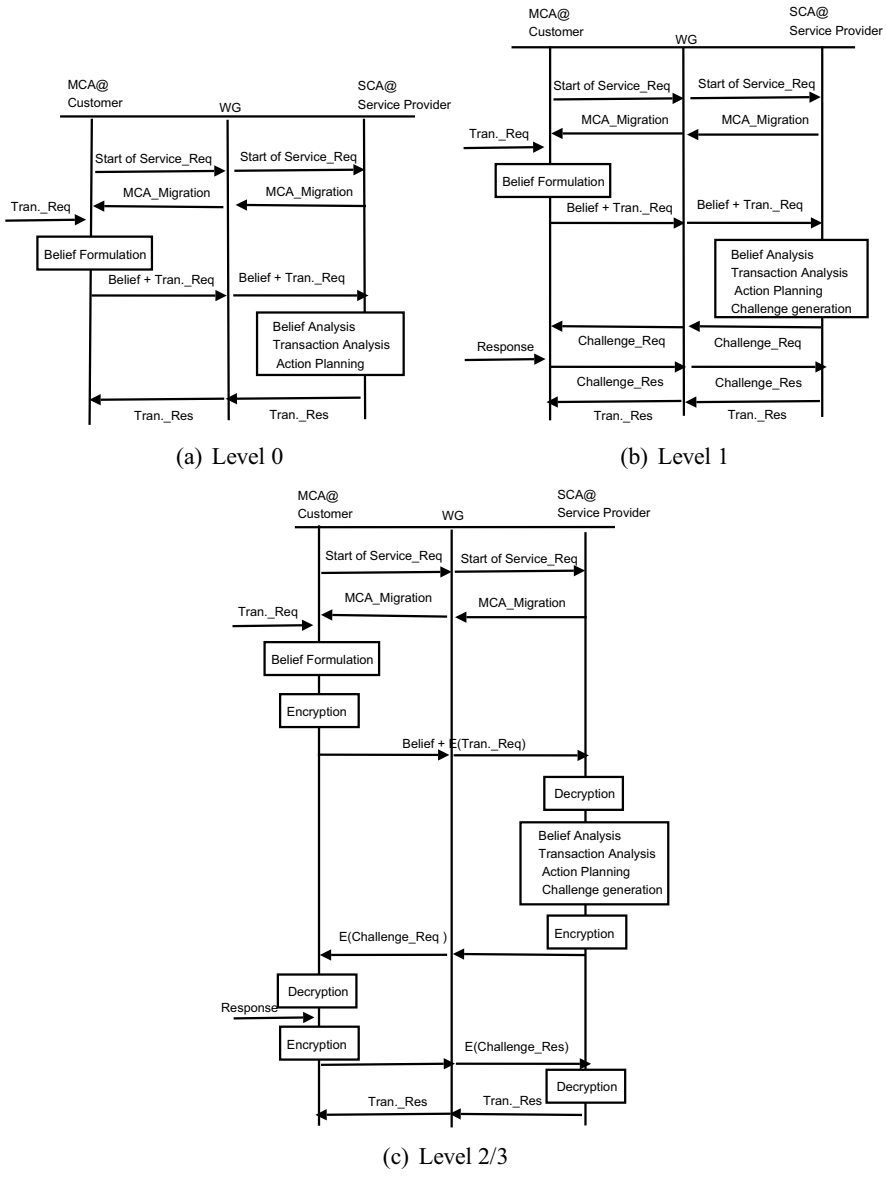
Where λ_l is the arrival rate of transactions of type l, and ${T_l}^i$ is the authentication delay per transaction of the l type, with the number of occurrence as i. We use the signaling diagrams shown in Fig. 3(a) - (c), to derive the delay for authentication in different sensitivity levels. A visiting customer sends a transaction request to a wireless gateway (WG), which is either an access point or base station. The WG relays the request to PMM-TBAS, the SCA migrates an instance of the MCA for beliefs generation to customer device. The set of time parameters are defined for convenient of description, shown in Table 1.

The, ${T_l}^i$ can be expressed as

$${T_l}^i = cT_x \tag{12}$$

Where c is the coefficient of T_x, denotes the number of such time parameters required for level l authentication. If the number of hops between customer and PMM-TBAS is N_h, then for various transaction sensitivity levels, the authentication delay per transaction are listed below.

For level 0 transactions, the T_{ap} is negligible, since no authentication actions are



(a) Level 0 (b) Level 1

(c) Level 2/3

Figure 3: Signaling diagrams

planned for these transactions, irrespective of the behaviors exhibited by the customer.

$$T_0{}^i = \ 4N_h(T_{pr} + T_{tr}) + T_{bf} + T_{ba} + T_{ta} + T_{ap} \quad ;i \geq 1 \tag{13}$$

Table 1: Authentication time parameters

Symbol	Description
T_{pr}	Message propagation time on one hop
T_{tr}	Message transmission time on one hop
T_{bf}	Belief formulation time by MCA
T_{ba}	Belief analysis time by SCA
T_{ta}	Transaction analysis time by SCA
T_{ap}	Action planning time by SCA
T_{cg}	Challenge generation time by SCA
T_{enc}	Time for encryption
T_{dec}	Time for decryption

For level 1 transactions, additional hops are required for challenge and response transmissions, during the first occurrence of these transactions, and when the customer shows the suspicious behaviors. Otherwise the level 1 transactions authentication delay is same as level 0 transactions. The challenge generation will introduce additional delay during authentication.

$$T_1{}^i = \begin{cases} T_0{}^i + 2N_h(T_{pr} + T_{tr}) + T_{cg} & \text{;if } i = 1 \text{ or Suspicious} \\ T_0{}^i & \text{;Otherwise} \end{cases} \tag{14}$$

For level 2/3 transactions, the number of hops remains same as that of level 1 transactions, but there is an additional delay of three pairs of encryption and decryption operations in case of first appearance of level 2/3 transactions or when the customer is suspicious. Otherwise the authentication delay remains same as level 0 transactions with an additional delay of one pair of encryption and decryption.

$$T_{2/3}{}^i = \begin{cases} T_1{}^i + 3(T_{enc} + T_{dec}) & \text{;if } i = 1 \text{ or Suspicious} \\ T_0{}^i + T_{enc} + T_{dec} & \text{;Otherwise} \end{cases} \tag{15}$$

The arrival rate of level l transactions, i.e., λ_l, is given by,

$$\lambda_l = \lambda_u P_l \tag{16}$$

The arrival of transactions from customer is considered as a Poisson process with average rate λ_u, with the PDF of the transactions inter-arrival time, which is denoted as

$$f_A(t) = \lambda_u e^{-\lambda_u t} \tag{17}$$

The P_l is the probability of occurrence of level l transactions. By considering a particular time interval *(t, t+Δt)*, the number of level l transactions appearing in this interval is given by, *I(t,t+Δt)*. Since we assume the transaction arrival rate is a Poisson process, the P_l is given by,

$$P_l = \int_0^\infty P[I(t, t + \Delta t) = 1] = \int_0^\infty \lambda_u \Delta t e^{-\lambda_u \Delta t} \tag{18}$$

Average authentication cost

The authentication cost is defined as the sum of signaling load and processing load for cryptographic techniques during each authentication operation. The average authentication cost C_l, is defined as the sum of the authentication cost over a number of authentication requests per unit time at transaction level l, which is given by,

$$C_l = \sum_\beta \lambda_\beta \Big[{C_\beta}^{(s)}(l) + {C_\beta}^{(p)}(l) \Big] \tag{19}$$

Where β takes the values based on the deviation factor value generated by *Belief analyzer* during belief analysis. The $\beta = 1$, if the deviation factor is < 0.5, $\beta = 2$, if the deviation factor is between 0.5 - 0.7, and $\beta = 3$, in case of deviation factor is > 0.7. The signaling load and processing load of cryptographic techniques are given by ${C_\beta}^{(s)}(l)$ and ${C_\beta}^{(p)}(l)$ respectively, and values of these parameters are dependent on β and l. The arrival rate of transactions from the user type β is defined as λ_β.

For convenience of analysis, we define a set of cost parameters as shown in Table 2. The transmission costs, ${C_\beta}^{(s)}(l)$, can be derived using the signaling dia-

Table 2: Authentication cost parameters

Symbol	Description
c_s	Transmission cost on one hop
c_p	Encryption/decryption cost on one hop
c_v	Verification cost at an authentication server
c_{us}	A pair of encryption and decryption cost for a value
c_g	Key generation cost
c_{ts}	Transmission cost for a key to other communication identities

grams in Figs. 3(a) - (c), as follows

$$C_{\beta}{}^{(s)}(l) = m_{\beta,l}c_s \tag{20}$$

Where $m_{\beta,l}$ is the number of hops by which the entire authentication process passes for particular type of user β, and the particular transaction sensitivity level l. When l=0, all the type of users transactions requires $4N_h$ hops and, when $l > 0$ additional $k*2N_h$ hops are required for transmitting the challenge and receiving the response, where k is the number of times the challenge is generated.

Similar to the analysis of $C_{\beta}{}^{(s)}(l)$, by using signaling diagrams in Figs. 3(a) - (c), the $C_{\beta}{}^{(p)}(l)$ can be written as

$$C_{\beta}{}^{(p)}(l) = \vec{n}_{\beta,l}.\vec{x}_p \tag{21}$$

Where, $\vec{x}_p$ is a vector defined as; $\vec{x}_p^T = [c_p, c_v, c_{us}, c_g, c_{ts}]$ and $\vec{n}_{\beta,l}$ is the vector denoting the corresponding number of costs to be considered during one authentication. The vectors $\vec{n}_{1,0} = \vec{n}_{2,0} = \vec{n}_{3,0}$ = [0,0,0,0,0], indicates for level 0 transactions there is no additional processing cost. The vectors $\vec{n}_{1,1}= \vec{n}_{2,1}= \vec{n}_{3,1}$= [0,1,0,0,0], one verification cost at PMM-TBAS is involved for level 1 transactions if the customer is *NORMAL;* otherwise, [0,k,0,0,0], k number of verification costs are involved, where k is the number of times the challenge is generated. The vectors $\vec{n}_{1,2} = \vec{n}_{2,2} = \vec{n}_{3,2} = \vec{n}_{1,3} = \vec{n}_{2,3} = \vec{n}_{3,3}$ = [$4N_h$,1,3,1,1], for level 2 or level 3 transactions if the customer is *NORMAL;* otherwise, it is $[k * 4N_h, k, 3k, k, k]$.

6. Simulation

Simulation Environment

The proposed authentication scheme has been tested on hybrid wireless testbed. Various mobile devices used in testbed includes Samsung X10 Laptop, HP iPAQ PDA with Bluetooth, and GSM/GPRS connectivity and CDMA enabled mobile phone. A PMM touring service system having 30 different transactions distributed among various authentication levels are implemented. These transactions includes: *place selection, traveling options selection, restaurants selection, reservation, purchasing tickets, etc.* The belief database is established for 100 PMM users.

Results and discussion

The effects of traffic pattern on the authentication delay at different sensitivity levels of transactions are demonstrated in Fig. 4. It is observed that the delay is proportional to the transactions arrival rate λ_u, since the variables λ_l (l =0,1,2,3) are proportional to λ_u. Higher the sensitivity of transactions more is the authentication delay.

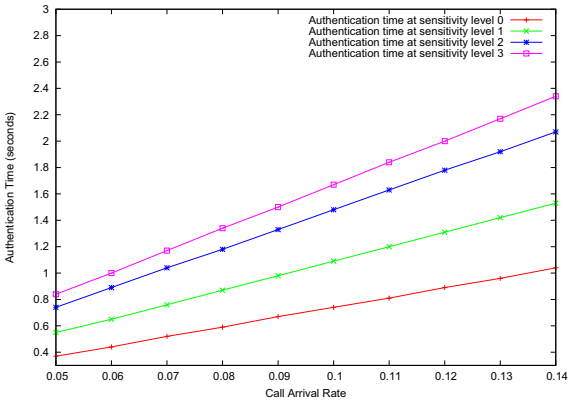


Figure 4: Authentication time vs. transactions arrival rate.

With the given transactions, we have plotted the average security cost in both PMM-TBAS and a typical session based security scheme, shown in Fig. 5. Since PMM-TBAS uses security algorithms only during type 2 and type 3 transactions it's average security cost is less, as compare to a session based scheme, which applies security algorithms for all transactions irrespective of the type of transaction going on.

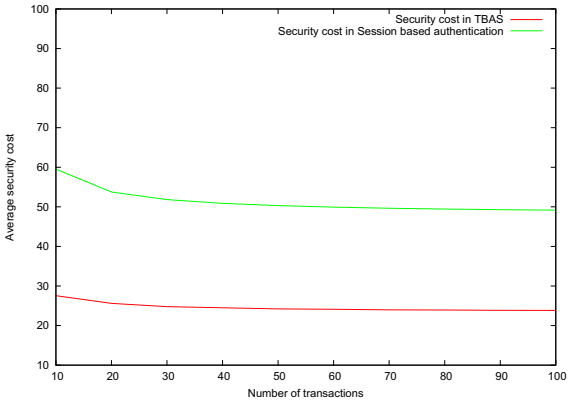


Figure 5: Average security cost in PMM-TBAS and session based scheme

Given a set of transactions, the Fig. 6, shows the plots on average authentication delay computed for both mobile IP and proposed PMM-TBAS without handoff and with handoff situations. For the simulation purpose, we have fixed the arrival rate of various type of transactions as, $\lambda_0 = 0.5$, $\lambda_1 = 0.3$, $\lambda_2 = 0.15$, and $\lambda_3 = 0.05$. The PMM-TBAS schemes naturally has additional delays due

to transactions analysis, belief formulation, belief analysis, challenge, verification, etc.

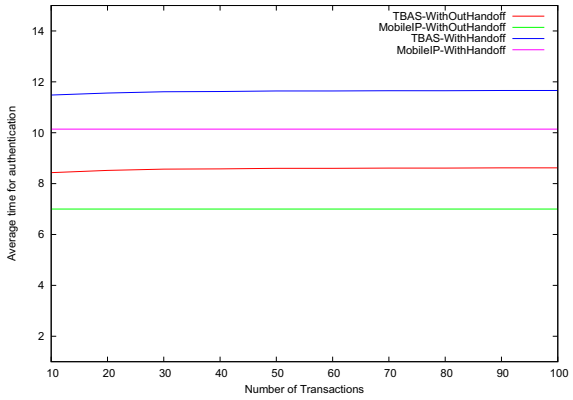


Figure 6: Average authentication delay of PMM-TBAS and MIP

With marginal addition of authentication delay, the PMM-TBAS detects many of the application level attacks which goes undetected under regular mobile-IP (MIP) schemes. Some of the simulated attack scenarios and the corresponding results from PMM-TBAS and MIP schemes are given as follows;

- **Scenario 1:** The attacker has stolen authentication identifiers of MU by successfully executing identity theft attacks, and using them to obtain the service.

  MIP: Successfully authenticates the attacker.

  PMM-TBAS: Authenticates the attacker, until his/her transactions become suspicious, then authentication challenges are dynamically created based on changes in sensitivity level of the transactions and beliefs.

- **Scenario 2:** The attacker is executing modification attack, by changing the contents of the transactions.

  MIP: No means to analyse transaction sensitivity levels, successfully authenticates the attacker.

  PMM-TBAS: Changes in transaction sensitivity levels are analyzed, and corresponding authentication challenges are created dynamically before committing the transaction.

- **Scenario 3:** Changes in attacker behaviors, for example, change in behaviors from normalcy to urgency.

  MIP: No means to recognize the changes in user behaviors, therefore attack becomes successful.

  PMM-TBAS: The user behavior analysis produces belief on urgency, which leads to high belief deviation factor, as a result authentication challenges are created dynamically.

7. Conclusions

In the proposed PMM-TBAS, the authentication process is continuous through out the session, it is not dependent only on the first time successful verification of authentication identifiers. The authentication procedure is not static, it keeps the changing sensitivity levels of transactions and beliefs deviation in order to propose the authentication challenges whenever required during the session. The scheme would be watchful from the beginning for a mischievous user whose track history is very bad. The scheme is pro-active in terms of sensing suspiciousness and blocking the critical transactions from execution, so that the unexpected behaviors of genuine users are handled with minimum interruptions.

References

[1] B. S. Babu and P. Venkataram. Transaction based authentication scheme for mobile communication: A cognitive agent based approach. In *Proceedings of the 3rd International Workshop on Security in Systems and Networks(SSN 2007), In conjunction with IPDPS 2007*.

[2] B. S. Babu and P. Venkataram. An authentication scheme for personalized mobile multimedia services: A cognitive agents based approach. In *Proceedings of Future Generation Communication and Networking(FGCN 2007)*, Dec. 2007.

[3] S. Boll, J. Krosche, and A. Scherp. Personalized mobile multimedia meets location-based services. In *Proceedings of the Multimedia-Informations systems workshop of the 34th Annual Meeting of the Germany Society for Computing Science*, pages 64–69, Sept. 2004.

[4] Y.-F. Chen, H. Huang, R. Jana, S. John, S. Jora, A. Reibman, and B. Wei. Personalized multimedia services using a mobile service platform. In *Proceedings of the IEEE Wireless Communications Networking Conference*.

[5] Z. Cui, A. Karmouch, R. Impey, and T. Gray:. Approaching secure communications in a message-oriented mobile computing environment. *Multimedia Tools Appl.*, 13:147–163, 2001.

[6] H. Harroud, M. Ahmed, and A. Karmouch. Policy-driven personalized multimedia services for mobile users. *IEEE Transactions on Mobile Computing*, 2:16–24, 2003.

[7] http://sourceforge.net/projects/agentfactory.
[8] A. Scherp and S. Boll. Generic support for personalized mobile multimedia tourist applications. In *Proceedings of the 12th ACM Int. Conf. on Multimedia*, pages 178–179, Oct. 2004.
[9] R. Seidl, F. Berger, S. Kapellaki, T. Frantti, E. Rukzio, J. Hamard, and N. B. Melazzi. The simplicity project: Personalized and simplified communication spaces for mobile users. In *Proceedings of IST Mobile and Wireless Communications Summit 2004*.
[10] K. Tanaka, M. E. Kounavis, and A. T. Campbell. Automating the creation of personalized mobile multimedia services using cellware. In *Proceedings of the 10th International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV' 2000)*, Aug. 2000.
[11] M. Wagner, W.-T. Balke, R. Hirschfeld, and W. Kellerer. A roadmap to advanced personalization of mobile services. In *Proceedings of the 10th Int. Conf. on Cooperative Information Systems (CoopIS) Industry Program*, 2002.
[12] Z. Yu, X. Zhou, D. Zhang, A. Lugmayr, and Z. Yu. A ubiquitous personalized multimedia service model based on fsm. In *Proceedings of the International Conference on Information Technology: Coding and Computing, 2005. ITCC 2005*.

AUTHORS

Pallpa Venkataram received his Ph.D degree in Information Sciences from the University of Sheffield, U.K.in 1986. He is currently a Professor of Electrical Communication Engineering with Indian Institute of Science, Bangalore, India. Prof. Pallapas research interests includes protocol engineering, wireless networks, network management, computational intelligence applications in communication, mobile computing security and multimedia systems. He is a Fellow of IEE (England), Fellow of IETE(India) and a Senior member of IEEE Computer Society. Dr. Pallapa is the holder of a distinguished visitor diploma from the Orrego University, Trujillo, Peru. He has published over 150 papers in International/national Journals/conferences.

B. Sathish Babu received his bachelors and masters degree in computer science and engineering from Bangalore university. From 2005 he is a research scholar in PET unit, department of Electrical Communication Engineering in Indian Institute of Science, Bangalore, India. His research interests includes intrusion and fraud detection systems for mobile commerce environment, mobile communication security, and application of cognitive agents in proposing dynamic transaction-based authentication system for mobile communications.