Transaction Based Authentication Scheme for Mobile Communication: A Cognitive Agent Based Approach

B. Sathish Babu and Pallapa Venkataram

PET Unit, Electrical Communication Engineering,
Indian Institute of Science, Bangalore, India.
Email:{bsb,pallapa}@ece.iisc.ernet.in

Abstract

The vulnerable air interface, device level constraints, and insecure encryption techniques of wireless networks have naturally increased the chance of attacker obtaining users information fraudulently. Most of the existing authentication systems for mobile communication principally depends on the strength of authenticating identifiers. Once the client who may be genuine or an attacker, successfully proves the possession of the identifiers the system accepts all the transactions of a session under single risk level, which is the most important point of vulnerability. We propose a novel Transaction Based Authentication Scheme(TBAS) for mobile communication using cognitive agents. The proposed approach intensifies the procedure of authentication by deploying authentication scheme based on the transaction sensitivity and client's transaction time behaviors. The TBAS provides effective authentication solution, by relieving the conventional authentication systems, from being dependent on only the strength of authentication identifiers. Additionally the transaction time behavior analysis by cognitive agents provides rational approach towards establishing the legitimacy or illegitimacy of the mobile client. The method has been simulated with different applications over in-house established wired and wireless networks. The Agent Factory framework is used for cognitive agents generation and communication. The simulation results are quite encouraging.

1 Introduction

The mobile communication and services over emerging wireless technologies provides anyone, anytime and anywhere access. The increased importance in mobile telecommunication and dominance of data communication promoted large segment of users to accept the mobile data communication as a part of their day-to-day activities.

However, the wireless medium has certain limitations over the wired medium such as open access, bandwidth limitations, complex system functioning, power confinement, and relatively unreliable network connectivity. These limitations make it difficult although possible to provide security features such as authentication, integrity and confidentiality. The wireless networks and the current generation of 3G networks have a packet switched core which is connected to external networks such as the Internet[4]; making it vulnerable to new types of attacks such as denial of service, viruses, worms, channel jamming, unauthorized access, eavesdropping, message forgery, message reply, man-in-the-middle attack, session hijacking, etc., that have been used against the Internet. Out of many security issues of mobile communication, this paper is focused on designing effective, dynamic and intelligent decision based authentication technique for mobile communication with respect to the transactions of the communicating parties.

1.1 Authentication

The primary aim of an authentication protocol is "verifying the linkage between an identifier(usually claimed by the individual, but sometimes observed) and the individual[6]." The introduction of many value added services in mobile world, has triggered exorbitant growth of mobile users population, many of these services demands for stringent authentication mechanism to ensure the right people are using the network and services. The authentication techniques are mainly classified into three categories[9]: Application level authentication, device level authentication and network level authentication.

The user centered design and human psychology, are the critical considerations while designing effective authentication and privacy schemes[6]. The human strengths and

1-4244-0910-1/07/$20.00

limits will become bottleneck for the complexity of the authentication systems. Bruce Schneier, a renowned cryptographer, have opinioned that, analyzing transactions during communication, will make the existing two-factor authentication schemes more robust, instead of only focusing on designing the strong identifiers. The approach of making authentication identities less useful, looks promising for mobile communication security because of many limitations of the wireless networks. The mobile transaction authentication is considered as one of the possible trend of mobile services[3], which enables a strong authentication at a transaction level based on the sensitivity of transaction, during the real time execution of mobile services.

1.2 Mobile transactions

The tasks performed by users in mobile environments are categorized into two types[1]: transactional tasks and information retrieval tasks. The transactional tasks updates database whereas information retrieval tasks are limited to browsing and searching activities. In the context of mobile computing, the mobile transactions(MTs) are, "transactions whose execution environments involve mobile affiliations. Any host in a mobile affiliation can initiate mobile transactions[8]." The research community has proposed many models for MTs to name a few[10], *Clustering, Two-tier replication, Pro-motion, Reporting, Semantics-based and Prewrite.* These models generally classify the MTs into two categories; the fixed host transactions and mobile host transactions. In the context of this paper, we assume the fixed host transactions refers to authentication services with large databases and software systems usually available on base station or on the cluster head mobile nodes. The mobile host transactions works with tentative versions of the data using compact software placed either on the service provider infrastructure or on the mobile device itself. The mobile transactions have a range of activities like; *searching; payments; personalized data service; educational; commerce; health care services; and so on.* The security requirements for these activities differs from one to other, and with in an activity the security requirement varies from one transaction to another.

1.3 Proposed authentication scheme for mobile transactions

The TBAS uses two types of cognitive agents: Mobile Cognitive Agent(MCA) and Static Cognitive Agent(SCA), which are secured with respect to their construction and inter communication(the discussion on agents security is out of scope of this paper). The total authentication scheme is distributed into two logical parts; the MCA part and the SCA part. The SCA creates MCA and sends to respective client, when a client needs to be authenticated, the MCA generates beliefs over client transactions by observing various transaction time behaviors. The SCA is used to dynamically generate authentication requirements, based on the sensitivity of mobile transactions and the changing belief on a client. The SCA could be deployed at various service points, like base stations and distributed authentication servers in case of infrastructure based wireless networks and on the cluster head mobile nodes in case of infrastructure-less(i.e., cluster based mobile adhoc) wireless networks. The challenge/response protocol has been incorporated to counteract, some common attacks such as; transaction interruption, transaction modification and transaction fabrication.

1.4 Organization of rest of the paper

The rest of the paper is organized as follows, section 2 provides some related work on the topic, section 3 gives some of the definitions, terminologies and concepts used in the paper, section 4 discusses the categorization of transactions based on authentication levels, and functioning of proposed system, section 5 provides simulation results including identification of some attacks, and finally section 6 draws conclusions.

2 Related works

Chen [2] proposed, a new authentication scheme for accessing contents, services and applications in both mobile device and Internet. The services and applications are divided into four groups according to their importance: extremely confidential group, very confidential group, confidential group, and free accessible group. The authentication usage levels are used to access the items in the four groups; The scheme doesn't made any attempts to categorize transactions happening in a particular group, as a result of this transaction based attacks are still possible. Killoran [7] suggested, a secured financial transaction architecture for wireless networks. The proposed SWiFT system includes the following three key components: a consumer e-card, a bank server(or banking agent server), and a merchant terminal. This approach claims the security risk has been reduced due to the device must only establish one secure channel and the bank has centralized control of all network connections. The main limitation of the scheme is pre-formated architecture, lack of flexibility, and the attacks using the compromised e-cards are difficult to determine. In some cases the mobile SMS channel is used to transfer to the users nominated handset either; one time passwords to enable user logon, and transaction summary information and authorization codes to enable transaction authorization.

The serious limitation of this scheme is, this authentication solution works provided the user is within mobile service range and the handset supports SMS.

3 Definitions

In this section we define a various terminologies used in the paper, in the context of cognitive agent based authentication.

3.1 Behaviors

The behaviors refer to the actions or reactions of a client while formulating and executing transactions; e.g., repeated login attempts and suspicious use of forget password options are the common behaviors of service intruder. The identification of behavior is based on collection of various temporal and symptomatic parameters during the service usage, e.g., *Time of transaction, Location, Network-ID, Device-ID, Type of transaction, Duration of transaction, Login attempts, Speed of data entry, etc.* The Suspicion Factor(SF) for each behavior is formulated as a function on values of the corresponding parameters, which is given by;

$$SF_{beh_i}({p_1}^{beh_i}, {p_2}^{beh_i}, \ldots, {p_m}^{beh_i}) \quad (1)$$

Where SF_{beh_i} is a function to generate suspicion factor for the behavior beh_i which is in the range 0 to 1, and the ${p_j}^{beh_i}$ represents the corresponding parameters.

3.2 Observations

In the current context the observation is the summarization of various suspicion factors of the observed behaviors during transaction execution, e.g., the behaviors *Taking a long time for entering transaction details, Making hurried entries, Repeated login failures, Improper time for transaction, etc.*, generate the observation as "Suspicious-user". The Criticality Factor(CF) of the observation is the summation of the suspicion factors of behaviors exhibited by the client, which is given by;

$$CF_{O_i} = \sum_{j=1}^{q} (SF_{beh_j}) \quad (2)$$

Where the CF_{O_i} is the criticality factor of i^{th} observation, which is computed using suspicion factors of q number of observed behaviors.

3.3 Beliefs

Primarily the "beliefs represents information about the world or an entity, perceptions received from the external world and execution of events update the beliefs[5]". The observations made on various behaviors will be deduced into beliefs. There exists pre-established relationships between observations and beliefs, these relationships are of types *"one-to-one, one-to-many and many-to-many"*. The Certainty Factor for a Belief(CFB) is a function of weighted sum of the criticality factors of the observations generated, given by;

$$CFB_{b_i} = \sum_{j=1}^{p} (CF_{O_j} * W_{O_j}) \quad (3)$$

Where the certainty factor of i^{th} belief which is having p number of observations is given by CFB_{b_i}. Following are some of the examples of beliefs used in proposed TBAS. On the network, the beliefs are: *Known, Unknown, Hazardous, Safe, etc.*; on the client transaction frequency, the beliefs are: *Frequent, Intermittent, Desultory, Meager, etc.*; on the client transaction behavior, the beliefs are: *Casual, Serious, Mischievous, Spammer, Intruder, Fraudster, etc.*.

3.4 Cognitive Agents

Cognitive Agents(CAs) are the agents with high reasoning capability to solve complex real world problems. The reasoning capabilities enable the agent to infer, rather than look up, its responses to percepts. CAs are often intentional, which means that their actions are motivated by specific goals and they store a symbolic representation of the world available. A cognitive act consists of three general actions[11]: 1. Perceiving information in the environment; 2. Reasoning about those perceptions using existing knowledge; and 3. Acting to make a reasoned change to the external or internal environment. In the proposed scheme, we made use of both static and mobile CAs.

3.5 Databases used

The following databases are used by various components of TBAS, during transaction authentication. 1. *Authentication database:* This database, at SCA side, is used to perform required authentication based on the sensitivity level of the transaction, it stores, "Authentication data set for each transaction level, account information, and some distinguishable physical attributes for critical transactions." 2. *Beliefs database:* This database, at SCA side stores, the beliefs along with established empirical values on required transaction parameters. The individual record is known as "Belief record" of a client. 3. *Transaction Log:* This database at SCA side maintains the detailed log of all the transactions conducted by the client of the system. 4. *Observations storage:* This is the temporary data storage available with MCA, for storing previously generated observations during the session. The content of this storage is used by Belief Formulator of MCA and Belief Analyzer of SCA.

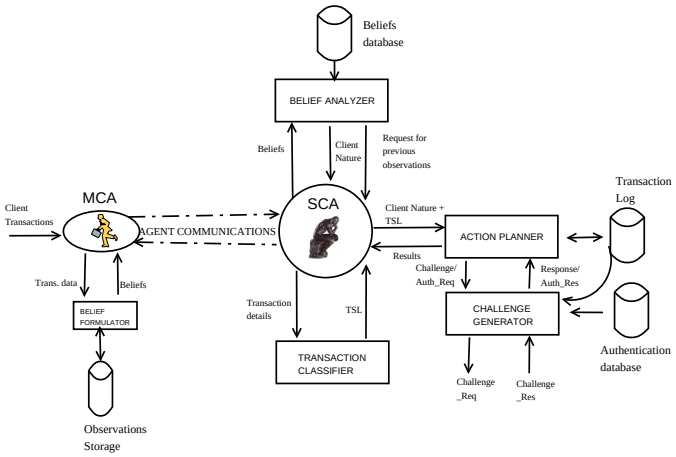


Figure 1. System Architecture

4 Proposed TBAS using CAs

The proposed TBAS deploys MCA at the client-side and SCA at the authentication server side. The MCAs gathers behaviors of the clients during every transactions execution, forms beliefs and send them to SCA for belief analysis and suitable authentication actions. In this section we explain the proposed categorization of mobile transactions and authentication data requirements, followed by the roles of MCA and SCA along with brief functioning of TBAS components and their algorithms.

4.1 Classification of mobile transactions

We classify the mobile transactions based on the degree of severity of information they handle, into four classes as shown in Table 1. For categorizing the transactions into various levels, it is essential to consider all the direct and indirect consequences laid out in the definitions of the levels[11]. The authentication services are need to consider the terms minor, significant and substantial in the context of the clients likely to be effected by misapplication of transactions. For example, if misappropriation of a service might result in risk to the clients personal safety, then the service must be allocated to level 3, even if potential financial loss or other consequences are minimal.

4.2 The TBAS

The TBAS architecture is shown in Fig. 1, consists of two cognitive agents and five functional components, the functioning of agents and various system components is explained below.

MCA

The MCA, migrates to a client with *Belief Formulator* logic by SCA, during the beginning of a session. The MCA communicates the generated beliefs along with transactions to SCA during every transaction. 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 observations stored. The functioning of MCA is given in Algorithm 1.

Algorithm 1 Working of MCA

```
1: Begin
2: Initialize the Observations Storage.
3: while Not end of client session do
4:     Accept transaction T.
5:     Pass T to Belief Formulator.
6:     Obtain belief from Belief Formulator.
7:     Send belief to SCA with T.
8:     if There is any request from SCA then
9:         Select observations from Observation Storage.
10:        Send observations to SCA.
11:    end if
12:    Periodically refresh Observations Storage
13: end while
14: End
```

Belief Formulator

The belief formulation component of MCA collects various temporal and symptomatic behavior parameters from the client transactions, and computes transaction time behaviors of the client and generates the observations. The beliefs are deduced based on the new observations and available observations from *Observations Storage.* The working of *Belief Formulator* is given in Algorithm 2.

SCA

The SCA co-ordinates the functioning of all the components at the authentication server, it is responsible for migrating MCA to client side and carrying out communications with MCA. Upon receiving the beliefs and transaction details from MCA, the SCA submits them to *Belief Analyzer* and *Transaction Classifier* respectively. The results obtained from these modules 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 beliefs from SCA and correlates them with established beliefs, in order to identify the amount of deviation. Based on the value of deviation factor, the *Belief Analyzer* produces three types of opinions on client nature, they are: *NORMAL-CLIENT, SUSPICIOUS-CLIENT and ABNORMAL-CLIENT*. The *Belief Analyzer* may also generate new beliefs to support belief analysis, especially when

Table 1. Authentication levels and transactions categorization

Level	*Authentication type*	*Transaction sensitivity*	*Examples Transactions*
0	Not required	Minimal/No damage	Product general information browsing, downloading free samples, browsing other client feedbacks, etc.
1	**Individual authentication based on:** SSN, Driving License number, Employee ID, pseudonyms, e-mail address, etc.	Minor damage	Request for technical information, requesting comparative statements, requesting after sales service options, placing low volume orders, making micro payments, etc.
2	**Identity authentication based on:** login-name, password, PIN, TAN, OTP, etc.	Signifi cant damage	Placing high volume orders, making macro payments, requesting purchase bills, requesting private information, making account transfers, etc.
3	**Attribute authentication based on:** Fingerprints, geometry of the human hand, pattern of tissues in the iris of the eye, etc.	Substantial damage	Collecting health reports, making advance large payments, etc.

Algorithm 2 Algorithm for Belief Formulator

1: Begin
2: Initialize B the beliefs set, BEH the behaviors set, and O the observations set.
3: **for** Each transaction T **do**
4: Let V= $\{v_1, v_2, \ldots, v_k\}$ is the set of values collected by agent for various temporal and symptomatic behavior parameters of transactions.
5: $\forall\, beh_i \in BEH$, compute SF_{beh_i}.
6: $\forall\, o_i \in O$, compute CF_{o_i}.
7: Select those o_i from O, which are not appeared before.
8: $\forall\, b_i \in B$, compute CFB_{b_i}; based on o_i and available observations.
9: Select those b_i from B, which crosses threshold of certainty and pass them to SCA.
10: Store newly generated o_i into *Observations Storage*.
11: **end for**
12: End

Algorithm 3 Working of SCA

1: Begin
2: **while** Not end of client session **do**
3: Accept Belief and transaction details from MCA.
4: Pass Belief to *Belief Analyzer.*
5: **if** There is any request from *Belief analyzer* for observations **then**
6: Fetch them from MCA.
7: **end if**
8: Pass transaction details to *Transaction Classifier.*
9: Pass client-nature and TSL obtained from above components to *Action Planner.*
10: **end while**
11: End

the client is turning out to be *SUSPICIOUS*. The early generated observations on client transactions could be obtained by sending request to SCA. The Algorithm 4 discusses the functioning of *Belief Analyzer.*

Algorithm 4 Algorithm for Belief Analyzer

1: Begin
2: Accept ${b_{new}}^i$ from SCA.
3: Compute $DEV_{b_i} = \beta({b_{new}}^i, {b_{old}}^i)$; where β is the belief deviation function.
4: **if** $DEV_{b_i} < 0.5$ **then**
5: Pass opinion as *NORMAL-CLIENT* to SCA.
6: **else if** $DEV_{b_i} > 0.5$ and $DEV_{b_i} < 0.7$ **then**
7: Pass opinion as *SUSPICIOUS-CLIENT* to SCA.
8: Generates additional beliefs (if required).
9: **else if** $DEV_{b_i} > 0.7$ **then**
10: Pass opinion as *ABNORMAL-CLIENT* to SCA.
11: **end if**
12: End

Transaction Classifier

Transaction classifier accepts transaction details from SCA and finds the Transaction Sensitivity Level(TSL). The TSL is generated by analyzing various transaction parameters, like, type of operation, type of data, sensitivity of data, volume of data, 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 opinion on client nature, the Action Planner performs the following actions. All the TSL(0) transactions are executed without any authentication by the system. If the transactions are appearing first time(TSL>0), it instructs the *Challenge generator*, to perform initial authentication for that transactions level. Other-

Algorithm 5 Algorithm for Transaction Classifier

```
1: Begin
2: Accept transaction details T from SCA.
3: Let OP is the operation requested by transaction T.
4: if OP is "READ" then
5:    Let INFO is the requested information to read.
6:    if INFO is public then
7:       TSL = 0.
8:    else if INFO is personal data then
9:       if personal public data then
10:         TSL=0
11:      else if personal private data then
12:         TSL = 1.
13:         /* More analysis on personal data – follows*/
14:      end if
15:   else if INFO is financial data then
16:      TSL = 2.
17:      /* More analysis on other readable items – follows*/
18:   end if
19: else if OP is "WRITE" then
20:   Let D is the target database for writing.
21:   if D is public then
22:      TSL = 0.
23:   else if D is personal record then
24:      TSL = 1.
25:   else if D is transaction Log. then
26:      TSL = 2.
27:      /* More analysis on other writable items – follows*/
28:   end if
29:   /* More Analysis on other transaction type – follows */
30: end if
31: Pass TSL to SCA.
32: End
```

wise, the action planner decides its future actions based on the value of client nature; as given in Algorithm 6.

Challenge Generator

This module is responsible for generating authentication challenges and counteracting challenges for attacks during transaction execution. The challenge generator uses the information stored in "Authentication database, Beliefs database and Transaction Log", to reason out the challenge question. The algorithm 7, shows the working of challenge generator and the Table 2 shows some of the sample challenges.

Algorithm 6 Algorithm for Action planner

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

5 Simulation

5.1 Simulation Environment

The wireless testbed has been established, to test the proposed authentication system. Various mobile devices used

Algorithm 7 Algorithm for Challenge Generator

```
1: Begin
2: if Transaction appearing first time then
3:    Create challenge using to perform initial authentica-
      tion of TSL.
4: else if Client-nature is SUSPICIOUS then
5:    Create challenge using Authentication data set of
      TSL.
6: else if Client-nature is ABNORMAL then
7:    Create challenge using Transaction Information.
8: end if
9: Validate the response obtained from client.
10: if Response is correct then
11:    Send "Success" to Action planner.
12: else
13:    Send "Failure" to Action planner.
14: end if
15: End
```

Table 2. Sample challenges

TSL	*Example Challenge*
1	Mention your nick name as entered during registration? What is your SSN? What is your employee ID?
2	Which is your favorite day of purchase?
3	What is the name of nominee in your account? , Which is your favorite electronic company?, Mention the month, when you last visited this service?

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 Access Point AiroNet 1200 series gateway is used for wireless networks and one of the local CDMA/GSM mobile service for cellular networks.

5.2 Creation of Cognitive Agents

The Agent Factory System(AFS) environment is used for creating cognitive agents, the AFS which is FIPA compliance, supports the belief modeling for the agent and implements agents communication through Agent Communication Languages (ACLs). The SCA and MCA are created with necessary datastructures and programs. The predicate based datastructure is used for representing the beliefs. For the simulation purpose, the belief database is created based on three parameters; delay between transactions, transaction value and transaction location. The belief formula used to represent individual belief of agent 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 will be reasoned.

5.3 Simulation Procedure

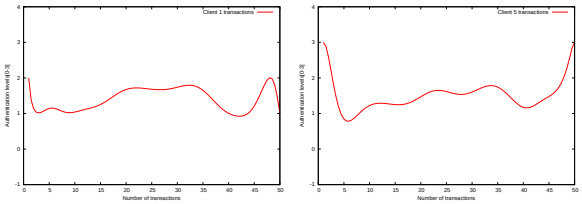
For the simulation purpose we considered a mobile service, which has 30 different transactions distributed among various authentication levels, ranging from no-authentication to physical attribute authentication. The belief database is established for 100 mobile clients who are using the given mobile service. The authentication database is created with all the necessary attributes. The normal mobile transaction scenario between mobile client and the authentication server has been simulated first, in which the mobile client connects to SCA through MCA for transaction executions. In the normal scenario the authentication challenges and transaction based challenges have been generated over the changes in sensitivity levels of transactions and client behaviors. In our attack model, we have injected the attack traffic into the stream of mobile transactions, by interrupting the session, intercepting and modifying the transactions; by varying the values of temporal and symptomatic parameters of transactions.

5.4 Results and discussion

To show the working of proposed system, consider the belief records of client 1 and 5: which are: *(1, Quick-decider, Lavish, Out-of-home)* and *(5, Slow-thinker, Poor-spender, Roamer)* respectively. Based on the values of the temporal and symptomatic parameters acquired during transaction execution, the MCA produces various observations like: *normalcy, urgency, slowness, lavishness, moderateness, poorness, Out-of-country, Out-of-home, Inside-home, etc.*. The transactions from the client 1 and 5 are generated randomly, with varied sensitivity levels and suspicions. The generated authentication levels for client 1 and client 5 are shown in Fig. 2(a) and Fig. 2(b) respectively.

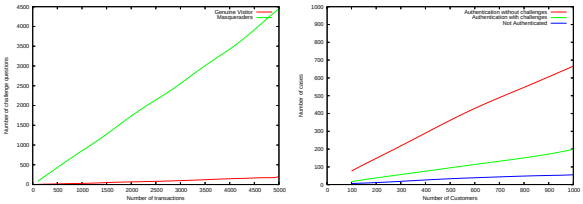
The Fig. 3(a), shows the results on generation of challenges for TSL(3) transactions by TBAS. It is observed that the genuine customers faced negligible number of challenges compared to masqueraders. The result of TSL(1) authentication shown in Fig. 3(b), which can be analyzed by the following factors; the number of genuine TSL(1) transactions authenticated without any transaction based challenges is significantly higher compared to the number of transactions authenticated with challenges. The number of genuine transactions not authenticated by the system is absolutely minimum, which shows the reduction in rate of false positives.

Consider a modification attack on client no. 1 and 5. During modification attack, the attacker will be modifying the content of the message transmitted from client to server. This process of blocking the client message at some intermediate point and later modifying it, will add additional delay between two successive transactions. This scenario has



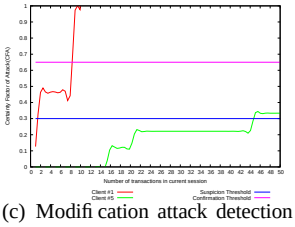
(a) Client 1 transactions (b) Client 5 transactions

Figure 2. Client transactions vs Authentication levels



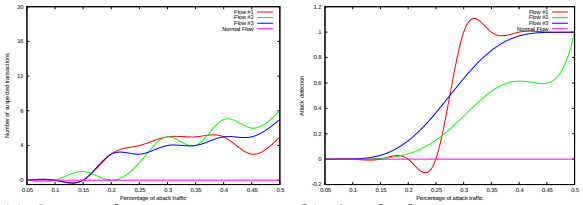
(a) TSL 3 challenge Questions vs clients

(b) Results of TSL 1 authentication



(c) Modifi cation attack detection results

Figure 3. Results



(a) Suspected transactions in various transaction fbws

(b) Attack detection in various transaction fbws

Figure 4. Suspicion and attack detection plots for various transaction flows with increased attack traffic.

been simulated by introducing additional delay between two successive transactions coming from the client. The results in Fig. 3(c), shows, the transactions session has 50 number of transactions from each clients. For the given test data the client 1 is shown as attacked, whereas the client 5 is shown as not attacked. The reason is by belief the client 1 is *Quick decider*, his/her transactions will not be delayed much. But the client 5 is *Slow-decider*, he/she spends more time between two transactions. Therefore the client 1 is declared as "Not-authenticated" and client 5 as "Authenticated".

The plots in the Figure 4(a) and (b), shows various transaction flows from group of clients. The attack traffic is introduced into flow with different percentages. The attack traffic is modeled by increasing the percentage of suspicion factor, which is calculated based on the delay between two successive transactions in a session. As a result of increase in percentage of attack traffic, more and more transactions enters into suspicion range. The attack is confirmed by the agent, only after the the certainty factor reaches 0.9.

6 Conclusion

The proposed TBAS using cognitive agents, is a new thinking towards dynamically and intelligently authenticating the mobile client based on transactions and transaction time behaviors. The scheme is *dynamic* by changing authentication requirements based on the sensitivity of transactions and *intelligent* due to use of cognitive agents; which will quickly identify the chances of attacks using belief modeling based on behaviors. We strongly feel that the rational approach towards authentication will address many of the existing weaknesses of conventional approaches of authentication.

References

[1] S. S. Chan, X. Fang, K. Brzezinski, Y. Zhow, S. Xu, and J. Lam. Usability for mobile commerce across multiple form factors. *Electronic Commerce Research*, 3, June 2002.

[2] H. Chen and Sivakumar. New authentication method for mobile centric communications. In *IEEE 61st conference on Vehicular Technology*, 2005.

[3] U. Forum. Development of spectrum requirement forecasts for imt-2000 and systems beyond imt-2000 (imt-advanced). *Report*, Jan. 2006.

[4] A. I. Gardezi. Security in wireless cellular networks. 2006.

[5] C. M. Jonker, J. Treur, and W. de Vries. Temporal analysis of the dynamics of beliefs, desires, and intentions. *Cognitive Science Quarterly (Special Issue on Desires, Goals, Intentions, and Values: Computational Architectures)*, 2, 2002.

[6] S. T. Kent and L. I. Millett. Who goes there?: Authentication through the lens of privacy. *The national academies press*, 2003.

[7] P. Killoran, F. Morgan, and M. Schukat. A new secure wireless fi nancial transaction architecture. In *International conference on Computer as a tool, EUROCON*, 2005.

[8] H. N. Lee and M. Nygrd. Mobile transaction system for supporting mobile work. In *IEEE 16th International Workshop on Database and Expert Systems Applications (DEXA05)*, 2005.

[9] E. Nielsen and S. Jacobs. A security model supporting the legacy userid:passphrase the authentication model that wont go away! *Draft*, 2002.

[10] P. Serrano-Alvirado, C. L. Roncancio, and M. Adiba. Analyzing mobile transactions support for dbms. In *12th International Workshop on Database and Expert Systems Applications*, 2001.

[11] T. Shimoda. A theory belief model for cognitive agents. 2006.