JIDR Journal of Interdisciplinary Research

Security in User- Assisted Communications

TONY ZHOU

Abstract

Today, companies called service providers enable communications and control the related infrastructures. However, with increased computing power, advanced wireless technologies and more standardized terminals, users in the future will be able to take more control of communications. In this paper, we define and discuss a disruptive communication model called User-Assisted Communications (UAC), which allows users to assist other users to establish communications, and propose a method for managing trust and security, which are the most challenging variables in UAC and must be addressed before UAC can be implemented successfully. A Social Network based Trust Establishment (SN-TE) is proposed for UAC implementation.

Keywords: Trust, Social Network, User, Service Provider, Digital Certificate, Authentication, Decision.

1. Introduction

Traditionally, service providers provide subscribers with communication services, including telephone and Internet access. Subscribers need to connect their devices (i.e. cell phones and computers) to service providers' network to establish communications. Since 1990's, wireless and packet data technologies have offered more advanced functions to support mobility and high-speed connections. With these capabilities, we envision a future where end users can provide services as well. This disruptive new model will benefit both the users and the service providers. In this paper, we propose a novel scheme for users to use their tangible (i.e. mobile phone, Wi-Fi Access Point (AP) and Internet connection) and intangible (i.e. identity, social relationship and reputation) assets to help others establish communications. The served users can save costs, and the serving users get credits for serving others. Also, the service providers' network resources can be utilized more efficiently. Figure 1 depicts the architecture of UAC including STAtion (STA), AP, Backhaul and Application Servers (for security, trust, billing, reputation, etc.).

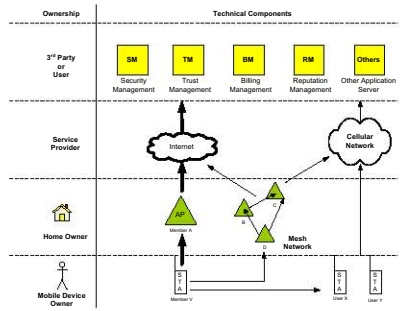

Figure 1 UAC architecture

In a service provider-controlled environment, the subscribers take the service provider as a trusted authority and rely on it to establish communications. However, with the UAC approach, the users who assist others may not have reputation. The rest of this paper is organized as follows. In Section 2, we explain the terminologies used in this paper. In Section 3, we classify UAC. A survey of related work is presented in Section 4. In Section 5, we discuss UAC implementation, including patent-pending solutions and how to solve the trust issue using SN-TE. Finally, we conclude the paper in Section 6.

2. Definitions and terminologies

User-Assisted Communications (UAC)

We define UAC as a framework to allow a user to assist another user and/or a service provider to establish communications. The word communication is a generic term in this paper that includes any types of data transmission, such as Internet access and file transfer, between two entities. Each individual has the capability to define his/her own AAA (Authentication, Authorization, and Accounting) [20] policy for offering services. We envision that UAC will challenge and compliment the current service provider controlled communications. Different types of UAC are classified in Section 3.

Serving user or node

A user or node that assists others to establish communications is called serving user or node.

Served user or node

A user or node that is assisted by others during communications establishment is called served user or node.

Trust

In social world, trust is the perception of people's confidence or faith in something or somebody. In scientific research, it may be quantified to different trust levels. Trust plays a critical role in UAC. User A may provide a class of service for User B and another class of service for User C based on his/her trust relationship with B and C.

Transitive trust

If A trusts B and B trusts C, A may trust C to some degree. This is called transitive trust. Trust can be either transitive or non-transitive depending on the judgments of people. People who accept transitive trust believe a friend's friend is likely to be a friend.

Trust path

In transitive trust, if a user trusts another user through other users, we say there is a trust path from a user to another user. For example, if A trusts B, B trust C and C trusts D, we have the trust path A → B → C → D. However, D may trust A from another path, such as D → E → F → A.

Social network

In many cases, people do not know each other directly. However, they could be socially connected through friendship, work relationship, blood relationship, community (i.e. club members and neighbors), or any combination of them. This type of intangible connection is called social network.

Social network based trust establishment (SN-TE)

In point-to-point communications, if two parties do not trust each other directly, they discover the possible connections between them through social network, upon which they make trust decisions separately. This is referred as SN-TE in this paper.

3. UAC classification

UAC covers a wide range of solutions for establishing communications. We classify it from four different angles.

1) Based on trust structure, we classify UAC as *hierarchical trust based UAC* and *non-hierarchical trust based UAC.* By hierarchical trust, we refer to the existence of an entity that is commonly trusted by all other parties. Hierarchical trust exhibits a tree structure. All the child nodes trust their parent nodes completely, and the trust is transitive. The node-to-node relationship in hierarchical UAC is relatively simple comparing with non-hierarchical UAC. However, a central authority (root) is not always available. In non-hierarchical trust UAC, there is no concept of levels and no commonly trusted party like the root of the tree. Each party acts autonomously as its own authority for making trust decisions. Thus, non-hierarchical structure exhibits a web structure.

Figures 2 (a) and 2 (b) depict the node-to-node relationships in hierarchical and non-hierarchical trust based UAC respectively. (The arrow points to the trusted person). Non-hierarchical UAC is more complicated than hierarchical UAC.

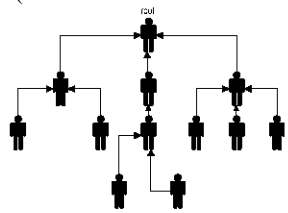

Figure 2 (a) Hierarchical trust UAC

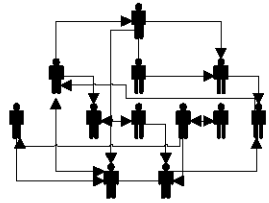

Figure 2 (b) Non-hierarchical trust UAC

In public key certification system, ITU X.509 [18] is the *de facto* standard for hierarchical trust, and PGP [18] is a popular solution for non-hierarchical trust.

2) Based on operation mode, we have *application mode UAC* and *transport mode UAC*. The application mode allows the serving user to offer services to a served user, while the transport mode only relays data as a dumb pipe. An application mode UAC is described in [1], which is a solution to transfer encrypted content from a serving user to a served user in a Peer-to-Peer (P2P) manner. Upon successful content transmission, a Digital Rights Management (DRM) controller releases the decryption key to the served user. An example of transport mode is that a serving user provides a served user with the unused bandwidth.

3) Based on the number of intermediate hops, we have *single-serving-user UAC* and *multi-serving-user UAC*. Between the served user and the target, if there is only one serving user to assist communications, we call it single-serving-user UAC. Figure 3 (a) shows a served user connects to only one serving user. The served user

trusts the serving user through Users 2, 3 and 4, and the serving user trusts the served user through Users 5 and 6. If there are multiple serving users between the served user and the target, we refer it as multi-serving-user UAC (Figure 3 (b)).

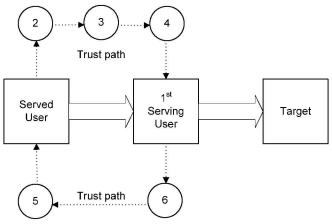

Figure 3 (a) Single-serving-user UAC

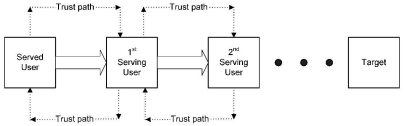

Figure 3 (b) Multi-serving-user UAC

4) Based on user and service provider involvement, we have *user-only UAC* and *joint UAC*. UAC can be established solely by individual users without any support of service provider's network. For example, a community can form a wireless network with user-owned access point installed in each household for intra-community communications. We call this user-only UAC (Figure 4 (a)). As the service providers have already established and managed backhaul network, such as Internet and wireless network, it appears more efficient to leverage the service provider's network for UAC when it is available. This is referred as joint UAC (Figure 4 (b)). Unlike wireless mesh network [19], which is a free data flow model, each node in UAC has the option to enable trust check using AAA technologies [20]. In Figures 4 (a) and 4 (b), Users B and C have enabled this option.

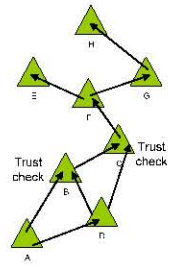

Figure 4 (a) User-only UAC

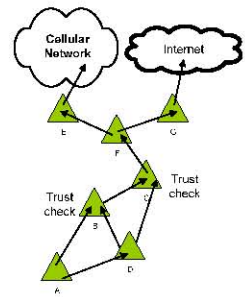

Figure 4 (b) Joint UAC

4. Related areas and works

UAC incorporates many aspects of the related technologies, including AAA [20], wireless mesh network [19], ad hoc network [11] and P2P [8]. In addition, UAC leverages the social behavior and asset of users, such as trust establishment, social network and reputation. UAC distinguishes itself on personalized trust management and authorization. We envision that advanced wireless technologies will provide people with capabilities to offer services to others. Many people may have the experience of connecting to neighbor's WiFi to access the Internet if the AP is not password-protected. UAC has been designed to provide users with strong control over establishing communications based individual's decision. UAC as a non-authority facilitated communication service has challenged the traditional authority-offered service. The efforts should be rewarded by the served users and the service providers who are benefited from cost saving and resource saving respectively.

Municipal WiFi network

Several cities in the U.S. have announced their plans to build

citywide WiFi networks for residential. In Philadelphia, Earthlink will provide the city government, schools and other entities with free wireless Internet access while charging about $20 per month for private access [3]. Comparing with UAC, municipal WiFi network is still a trusted authority-provided network.

Wireless mesh network (WMN)

WMN [19] allows data to be transmitted freely over any available resources. It can increase the network reliability as data can reach destination through different paths and a damaged intermediate node cannot stop the data flow from other nodes. But WMN still lacks efficient and scalable security solutions [19]. In UAC, each node is able to define its AAA [20] policy.

Ad hoc network

Without any infrastructure support, ad hoc networks [11] are self-formed for temporary connections of mobile nodes. IETF has formed a Mobile Ad hoc NETwork working group (MANET) to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies [22]. The key management schemes of ad hoc networks (with or without a trusted third party) have been summarized in [11]. These schemes can be adopted by UAC. In contrast to ad hoc networks, UAC allows users to offer a variety of services, such as file transfer [1] and location determination [2], and obtain credits in return.

Peer-to-peer (P2P)

P2P [8] has changed data distribution from a centralized model to a distributed model. P2P file sharing systems, such as Napster and Gnutella, emerge as a controversial technology enabling a user to retrieve content from other users rather than the original content owner. Mobile operators are better suited to solve some of the typical P2P issues because they have greater control over their subscribers [12]. A fully self-organized security scenario using asymmetric-key approach and symmetric-key approach has been discussed in [13]. In UAC, users can offer additional new services, such as paging [5], bandwidth sharing [2] and conference hub [7], leveraging their resources in a P2P manner.

Digital certificate

A digital certificate binds a user's public key to his/her identity with the certificate-issuer's digital signature. ITU X.509 [18] digital certification is based on hierarchical structure, while PGP (Pretty Good Privacy) [18] certification takes non-hierarchical structure. PGP has introduced two key attributes, validate level and trust level, for a user to determine the confidence level of another user's certificate and another user's certification capability respectively. We utilize

PGP for SN-TE implementation in this paper.

Small world phenomenon

First tested by social psychologist Stanley Milgram in 1967, small world phenomenon has attracted many researchers from social and computing areas. It suggests that people are connected through a short chain of acquaintances (six degree of separation) [21]. UAC is inspired and backed up by the small world phenomenon. The six degree of separation property makes SN-TE practical as it is very possible that a trust path exists between two people who do not know each other directly. There are several Internet web sites built for social relationship, such as Linkedin.com. In addition, the buddy-list server for Instant Messaging (IM) can also be enhanced for searching relationships [6].

Trust management

Trust is a function of context, identity, reputation, capability and stake, and also conditioned by social and cultural factors [14]. Different trust models and quantification methods have been discussed in [4] [15]. We summarize the properties of trust as follows:

- Trust is dynamic. It can be established, increased or decreased from time to time.
- Trust is self-maintained and subjective.
- Trust can be transitive or non-transitive depending each individual's believe.
- Trust has different levels. (i.e. complete trust and marginal trust)

In Section 5, we discuss SN-TE using enhanced PGP and how to make trust decisions.

Mobile Bazzar (MoB)

MoB [2] has introduced an open market concept to promote fine-grained competition by decoupling infrastructure providers from service providers. We share the same vision that any device can autonomously advertise services and resell services to other users. The MoB paper [2] has discussed the roles of reputation management and accounting in no-trust model. In that paper, the authors express the security concern in open, collaborative environment and state that MoB does not explicitly address data security and integrity issues. In this paper, we include trust and security solutions for UAC.

5. UAC implementation

UAC can be formed in many different ways. A proper implementation can improve resource efficiency and increase customer loyalty. We have designed three patent-pending solutions (outlined below) that allow the served users to obtain services from serving users.

1) When an out-of-coverage user is called, the MSC (Mobile Switching Center) may page the user. Upon the cellular network paging timeout, the MSC requests the serving user(s) to relay a new paging message to the served user through a short-range wireless connection, such as WiFi. (Figure 5) The served user receives the paging message from the serving user and then establishes a connection to the serving user, who is connected to the service provider's network [5].

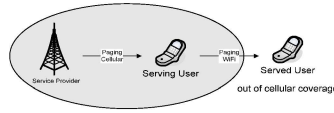

Figure 5 Paging extension

2) Instant Messaging (IM) is a very popular service. Users create their buddy-lists on a server, and communicate with the buddies by text messaging or voice calls. A buddy-list server can be utilized to search for the common friends of the served user and the serving user. [6] provides a solution to allow a served user to access a serving user's wireless AP because they can find a common friend from their buddy-lists (Figure 6).

Figure 6 Buddy-list based UAC

3) In a group call, each user needs to establish a separate reverse connection (from the user to the network) with a conference server. In the case that some of the group members are collocated, a user among them can serve as a hub to connect the surrounding users to the conference server. Figure 7 illustrates that the served users connect to the serving user through WiFi, and the serving user connects to the cellular network [7].

4)

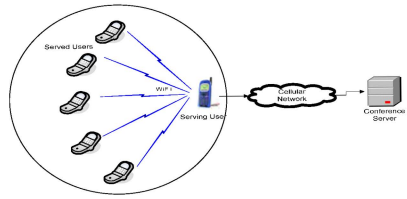

Figure 7 Mobile-bridged conference call

Many other UAC services may be discovered later. The rest of this paper focuses on the detailed discussion of a mobile originated one-hop transport mode UAC using SN-TE, which is based on non-hierarchical trust. Social network exists in different ways. In the following discussion, PGP is used as the method to construct SN-TE for UAC implementation.

A. PGP and its limitation

PGP was initially created for users to secure Internet Email, which is a one-way communication. It is widely accepted by the mass and recognized as a key contribution to the applications of cryptography. Any individual user can issue certificates to others based on his/her personal judgment. The person who issues certificates to others is also referred as introducer. The introducer chains build a "web of trust". The CERT_DEPTH parameter is used to define the maximum certification chain length, but it is unsure how this is used in evaluating certificate validity. PGP only allows one introducer. (i.e. in Figure 8, User 2 introduces User 3 to User 1.) The algorithm to evaluate the validity of public key is described in [16]. In other words, PGP has no capabilities for introducing other introducers [16]. This limitation does not support Social network, where chained introductions exist.

B. Enhanced PGP for SN-TE

We propose the following PGP enhancements for SN-TE to support UAC implementation.

1) Transitive trust is assumed between communication parties, including introducers.
2) Six degree of separation is used as the default value for CERT_DEPTH when searching common friends of two communication parties.
3) Multiple disjoint and/or joint trust paths are supported for trust evaluation.
4) Mutual trust between communication parties is supported.

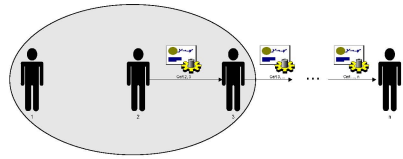

Figure 8 Social network based trust establishment (SN-TE)

C. Call flow

We assume User A and a Visitor (V) do not know each other. V explores the possibility to connect to the Internet via A's AP. The call flow in Figure 9 depicts how V's STA negotiates with A's AP using SN-TE in six stages. We also assume that A and V are able to obtain the needed certificates from a public PGP directory.

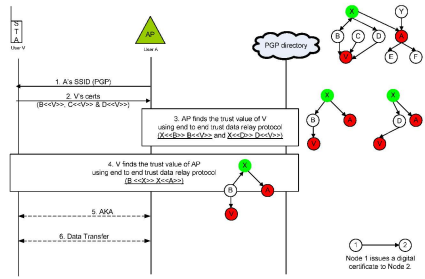

Figure 9 UAC call flow

(1) A broadcasts its Service Set IDentifier (SSID) and indicates that it accepts PGP certificates.
(2) V sends A its PGP digital certificates issued by B, C and D, which are denoted B <<V>>, C<<V>> and D<<V>> respectively.
(3) A trusts X as a CA (although A doesn't issue a digital certificate to X), but A doesn't trust C as a CA. So X<<B>> and X<<D>> are accepted; C<<V>> is ignored. With the end to end data relay protocol and decision making methods discussed in the Section D, E and F, A is able to determine whether it wants to provide V with UAC service or not.
(4) Similarly, V obtains B<<X>> and X<<A>> from the PGP directory on the Internet, and determines whether it wants A to provide UAC service or not. (We assume that A allows certificate search traffic to go through its AP for a short period of time.)
(5) If both A and V are willing to establish a connection, they perform public key based Authentication and Key Agreement (AKA).
(6) V sends secured data to the Internet through A's AP.

D. Single PGP certification path

In Figure 10, we assume that Node 1 needs to check the validity of Node J's public key before negotiating a connection with it, but Node 1 doesn't have the validity information stored in its public ring. So Node 1 needs to find a PGP certification path from Node 1 to J in order to collect the "opinion" from the intermediate nodes and then made a decision. The "opinion" includes the PGP validity level and trust level, which are two key attributes in PGP. (For simplicity, we ignore other factors that may affect decision in this paper.) The validity level reflects a person's confidence of another person's the public key ownership, and the trust level indicates the degree to which a person trusts another person's certification capability. As the two attributes are determined by each individual, they are deemed to be private. Section D1 describes a solution to relay the attributes from the intermediate hops to Node 1 with security and privacy protection. We refer the intermediate nodes as Node 2, …, Node i, Node i+1, … and Node J-1 as shown in Figure 10. Each node except J has the validate level and the trust level to the next hop. We further assume that each intermediate hop has the addressing information of the next hop and the previous hop, and only one path between Node 1 and J exists. [9] has described an algorithm to search for the shortest PGP certification path.

After a PGP certification search resulting in the validity and the trust level relayed back to Node 1 from each intermediate node on the certification path, Node 1 determines the validity of the target's public key based on the decision making methods that are proposed in Section F. $V_{i, i+1}$ and $T_{i, i+1}$ represent the validity level and the trust level Node i assigned to Node i+1 respectively.

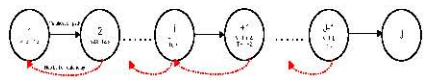

Figure 10 Single PGP certification path

D1. Hop-by-hop data relay method using IKE-SKEME [10]. We propose the following security requirements for hop-by-hop data relay, which refers to data transmission from Node i+1 back to Node i.

- User mutual authentication – adjacent hops must authenticate each other.
- Data confidentiality – private information, such as validate level and trust level, transmitted between hops cannot be decoded by eavesdroppers.
- Data authenticity (integrity) – ensure data is from the intended source and not altered during transmission.
- Privacy protection – a receiver cannot prove to a 3rd party that the received private information is from a certain sender.

With the requirements above, we propose to use the IKE-SKEME protocol [10] with some modifications for the hop-by-hop data relay. Figure 11 illustrates the scenario that A requests B to send B's data (validity level and trust level) on B's next hop (not shown), and how B responds to A.

Step 1. A selects a random number N_A and use B's public key to encrypt N_A and A's identity (A).
Step 2. B selects a random number N_B and uses A's public key to encrypt N_B, B's Data and B's identity (B) to provide data confidentiality. B also attaches a Message Authentication Code (MAC) for data authenticity ($K_0 = H(N_A, N_B)$).
A is assured that the data is from B, but A cannot prove it to a 3rd party because the message from B has no bearing of B's digital signature, and A can possibly forge the message by itself.
Step 3. A acknowledges B after it verifies the data is from B and not altered during transmission.

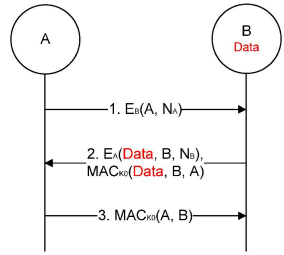

Figure 11 Hop-by-hop data relay

D2. End-to-end data relay. With the hop-by-hop data relay method described above, the validity levels and the trust levels of all the intermediate nodes on the certification path can be relayed back to Node 1 securely. The PGP digital certificates are also relayed back to Node 1 by the intermediate nodes. The example in Figure 12 self-explains how it works. (The immediate hop to the last node, Node 3 in the example, may only send back the validity level as the trust level is not needed by Node 1.)

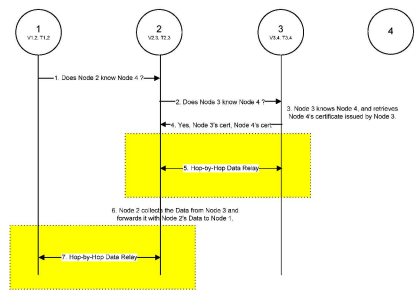

Figure 12 End-to-end data relay

E. Multiple paths

It is possible that two or more certification paths exist from one node to another node. The paths can be disjoint or joint as shown in Figure 13 and Figure 14 respectively. If the paths are disjoint like Path 1, …, Path i, …, and Path K in Figure 13, the data Node 1 obtained from each path is independent. Several researchers have proposed metrics for measuring the assurance provided by a set of paths. For example, Beth et. al propose a formula to calculate the result of combined direct trust value. The design criteria for these metrics are not widely agreed upon [4] [17]. Section F describes our trust decision-making proposal. If between two nodes, some paths have joint points (Figure 14), the decision-making method should be adjusted to reflect redundant information. We defer joint path to future discussions.

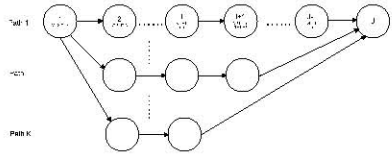

Figure 13 Multiple disjoint paths

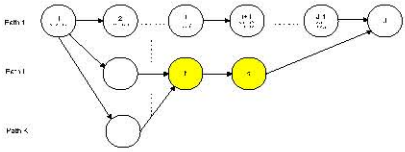

Figure 14 Multiple joint paths

F. Making decision

Many factors can influence in making decision, such as risk and reputation. Some people may be more open and optimistic and some others may be more conservative. This paper limits the discussion to using validity and trust level for making decision on a single path or multiple disjoint paths.

With the data collected from different nodes and paths, Node 1 can choose one of the proposed methods in Table 1 to decide if it trusts the legitimacy of the target's public key. Similarly, the target (Node J) can check the validity of the Node 1's public key. The certification path(s) from Node 1 to the target may differ from the path(s) from the target to Node 1. If both nodes accept each other's public key, further handshake will occur to establish secure communications.

In the following, we describe a multiplication solution for calculating the public key validity. For a single certification path *k* from Node 1 to J,

we multiply the validity levels $V_{i,i+1}$ and the trust level $T_{i,\,i+1}$ as follows.

$$V^k = (\prod_{i=1}^{J-2} V_{i,i+1} * T_{i,i+1}) * V_{J-1,\,J,}$$

where V^k is the end to end validity level Node 1 calculated for the certification path *k* starting from Node 1 and ending at Node J. If there are multiple disjoint paths (K) between two nodes, the validity value of each path may be calculated.

Node 1 uses the calculated validity value against a threshold (Table 1) it selects. If it is above the threshold, Node 1 trusts the target's public key. Otherwise, Node 1 has no confidence on the key. Table 1 has provided different types of thresholds for making a decision.

Table 1 Different types of thresholds

Threshold	Description	Condition
Optimistic Threshold (V1)	As long as there is a path with the validity level greater than V1, the public key of the target is considered as valid.	$\forall V^i > V1$, (i = 1, 2, …, *K*)
Average Threshold (V2)	It requires the average of all disjoint paths to be above V2 for the public key to be considered as valid.	$\frac{1}{K}\sum_{i=1}^{K} V^i > V2$
Strict Threshold (V3)	Each of the certification path needs to have an end-to-end validity level above V3 so that the public key is considered as valid.	All V^i > V3, (i = 1, 2, …*K*)
Aggregated Threshold (V4)	If the total validity value calculated from all disjoint paths is more than V4, the public key of target is assumed to be valid.	$\sum_{i=1}^{K} V^i > V4$

6. Summary and Future Works

In this paper, we have introduced the new concept of UAC and proposed a method to solve its trust and security issues. We believe that UAC will create win-win opportunities for the service providers and the end users. The service providers and the served users can reduce costs and improve the performance of services. And the serving users can also benefit from helping others. UAC is a disruptive model that challenges today's service provider-controlled communications. Our future works include UAC enhancements, simulation and prototyping.

7. Acknowledgement

We appreciate the feedback from Dr. Jiongkuan Hou, Technical Architect of Sprint Nextel, and Jason Schnellbacher, Consultant for Sprint Nextel.

8. References

[1] David J. Marples and Benjamin W. Falchuk, “Payment System for the Distribution of Digital Content Using an Intelligent Services Control Point”, United Statues Patent Application Publication Number: US 2006/0173784 A1 Pub. Date: Aug. 3, 2006.

[2] Rajiv Chakravorty et al, “MoB: A Mobile Bazaar for Wide-area Wireless Service”. MobiCom’05, August 28–September 2, 2005, Cologne, Germany.

[3] Joni Morse, “Philadelphia loses chief of Wi-Fi push to consulting firm linked to muni network”, RCR Wireless News, April 18, 2006.

[4] Michael Reither and Stuart Stubblebine, Authentication Metrics Analysis and Design”, ACM Transactions on Information and System Security, 2(2), 1999.

[5] Tong Zhou and David Mohan, “Method And System For Setting Up A Call To A Mobile Station Via Another Mobile Station”, Sprint Nextel pending patent.

[6] Tong Zhou, “Self-Organized Network Setup”, Sprint Nextel pending patent.

[7] Tong Zhou and David Mohan, “Method And System For Setting Up A Conference With A Mobile Station Via Another Mobile Station”, Sprint Nextel pending patent.

[8] Karl Aberer, Manfred Hauswirth, “An Overview on Peer-to-Peer Information Systems”, Workshop on Distributed Data and Structures (WDAS-2002), Paris, France.

[9] Computing shortest paths in WOTs (Web of Trusts), Henk P. Penning, http://www.cs.uu.nl/~henkp/henkp/pgp/pathfinder/doc/shortest-paths-in-wots.php.

[10] Colin Boyd and Anish Mathuria, “Protocol for Authentication and Key Establishment”, Springer, 2003.

[11] Hegland, A.M. et al, “A survey of key management in ad hoc networks”, IEEE Communications Surveys & Tutorials, Volume 8, Issue 3, 2006.

[12] K.R. Renjish Kumar and Heikiki Hammainen, “Peer-to-Peer Content Delivery over Mobile Networks: A Techno-Economic Analysis”, Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC 2005).

[13] Srdjan Capkun et al, “Mobility Helps Peer-to-Peer Security”, IEEE Transactions on Mobile Computing, Vol. 5, No. 1, January 2006.

[14] Daniel J. Essin, “Patterns of Trust and Policy”, 1997 New Security Paradigms Workshop Langdale, Cumbria UK.

[15] Asad Amir Pirzada and Chris McDonald, "Establishing Trust In Pure Ad-hoc Networks", the 27th Australasian Computer Science Conference, Copyright © 2004.

[16] Alfarez Abdul-Rahman, "The PGP Trust Model", http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs/pgptrust.html, 1996.

[17] Thomas Beth et al, "Valuation of Trust in Open Networks", Proceedings of the Conference on Computer Security, 1994.

[18] William Stallings, "Cryptography and Network Security: Principles and Practice", 2nd Edition, Prentice Hall, 1998.

[19] Akyildiz, I.F. and Xudong Wang, **"**A survey on wireless mesh networks", IEEE Communications Magazine, Volume 43, Issue 9, September 2005.

[20] D. Mitton et al, "Authentication, Authorization and Accounting Protocol Evaluation", RFC 3127, 2001.

[21] Duncan Watts, "Small Worlds: The Dynamics of Networks between Order and Randomness", Princeton, 1999.

[22] IETF Mobile ad hoc Works (Manet) http://www.ietf.org/html.charters/manet-charter.html