Short Paper: Can Your Phone Trust Your Friend Selection?*

Sebastian Trapp
Institut für Informatik
Freie Universität Berlin
14195 Berlin, Germany
sebastian.trapp@fu-berlin.de

Matthias Wählisch
Institut für Informatik
Freie Universität Berlin
14195 Berlin, Germany
m.waehlisch@fu-berlin.de

Jochen Schiller
Institut für Informatik
Freie Universität Berlin
14195 Berlin, Germany
jochen.schiller@fu-berlin.de

ABSTRACT

In ad hoc communication, data packets are relayed over several hops before reaching their destination. Spontaneous communication requires that nodes trust each other as communication can be intentionally disturbed or privacy compromised by the intermediate nodes. Establishing this trust relationship within a MANET without access to a central authority poses a challenge. In this work, we discuss the problem of ad hoc trust assignment and present an approach that helps to establish trust relationships between smartphones forming a MANET. Inspired by sociological insights we argue that data inherently available at mobiles can be used to define the social relationship of two individuals. Based on a preliminary measurement-based analysis we show that this data can give an initial estimation of trust between two users and their mobiles.

Categories and Subject Descriptors

C.2.0 [**Computer-Comm. Networks**]: General—*Security and protection (e.g., firewalls)*

General Terms

Security

1. INTRODUCTION

The increased usage of smartphones, equipped with numerous network interfaces, strengthens the trend to ad hoc communication. Transferring data via one or several neighboring devices, however, poses a security risk, since packet drops or even eavesdropping and data manipulation can occur. Hence, determining the trustworthiness of nearby nodes is an important precondition for ad hoc communication.

The use of authentication, the most common way to determine trust between two systems, may not always be possible. Central services may not be available to mobile phones at all times. In addition the distribution of pre-shared secrets between all mobile phones is not practical. Consequently, two smartphones that never met before require spontaneous, lightweight, and autonomous evaluation of mutual trust.

This work introduces a concept to evaluate the level of trust towards another phone based on data inherently available on smartphones. Our concept is inspired by sociological studies. Contact lists, containing telephone numbers and email addresses, as well as user IDs of Online Social Networks (OSNs) comprise information about the social network of the phone's user. By identifying mutual entries in contact lists of two users, their social relationship can be revealed. Assuming you assign a certain level of trust to a known person, this approach provides a measure for trust between technical devices on a social basis. Through sociological analysis we show that from technically observable features (e.g., call durations) conclusions about the social relationship of two individuals can be derived. Those insights can be extended to obtain an estimator of trust between devices.

Compared to other approaches dealing with the evaluation of trustworthiness of nodes in a mobile ad hoc network, our scheme utilizes only and specifically data inherent in mobile phones. In this paper, we argue that fundamental sociological findings from social network research (i.e., [1] and follow-up work) helps to reduce complexity in technical trust establishment. From a more general perspective, we believe that the introduced concept of socio-inspired security has some potential beyond trust establishment, e.g., with respect to the challenge of resource allocation [2]. The incentives of helping a friend are higher than the willingness to support a complete stranger with bandwidth and limited energy resources.

The remainder of the paper is structured as follows: In Section 2, we describe and analyze the general problem space in more detail including related work. Section 3 presents our concept for socio-inspired trust establishment between mobile phones. A preliminary real-world analysis shows the potential and challenges of our approach in Section 4. In Section 5, we discuss the concept with respect to practical open questions and outline a possible research agenda. We conclude with an outlook in Section 6.

2. PROBLEM STATEMENT

In mobile ad-hoc networks (MANETs), messages can in general be tapped, altered, or dropped by nodes along the path of the data to its target. Even with end-to-end encryption packet drops can still occur and prevent commu-

*This work is supported by the German Bundesministerium für Bildung und Forschung within the project SKIMS (http://skims.realmv6.org).

SPSM'11, October 17, 2011, Chicago, Illinois, USA.

nication. When smartphones form a MANET they might need to transfer personal or sensible data and thus have a vital interest in submitting data packets only to trustworthy neighbors.

2.1 Why Ad Hoc Communication for Mobiles

A mobile phone is equipped with several network interfaces, typically at least one for infrastructure-based and one for ad-hoc communication. Current developments in the context of mobile phone communication require spontaneous data exchange. They are motivated by two perspectives: (a) new application scenarios and (b) performance improvements.

Considering the tremendous number of mobile phones and the advantages of cloud computing, such devices may form a large virtual data center. Quite recently, the idea of crowd computing has been introduced, which uses opportunistic networking and the aggregated power of mobiles to allow for cheap, large-scale distributed computing [3]. Cooperative communication may also improve the protection of smartphones against disturbances that are initiated via the network infrastructure (e.g., denial of service attacks). If an alternative connection exists, a firewall extension can deactivate insecure paths as soon as a suspicious event raises.

In contrast to application-driven trends, multipath scenarios integrate an ad hoc network to improve the communication of a smartphone. A recent measurement study [4] shows that packet loss is the main reason for reduced throughput at smartpones. Limited radio coverage or the use of unstable wireless paths can be mitigated by the creation of an ad hoc network, which provides additional Internet access. Following the resource pooling principle, the IETF started the standardization of a multipath mechanism on the transport layer [5], which transparently bundle different communication channels to increase throughput. A first prototype for the Nokia N900 device is already available [6].

All of these scenarios require a (mobile) ad hoc network to extend mobile phone communication. Mobile ad hoc networks, however, pose the challenge of identifying trustworthy neighbors. Intermediate malicious nodes can tap, alter, or drop messages. Intentional packet drop cannot be avoided even with end-to-end encryption. Thus, to advance trusted communication in MANETs of mobile phones, a method is needed that allows for spontaneous, lightweight, and autonomous evaluation of trust.

2.2 How to Assign Trust

When a phone establishes contact to another device for the first time, it can set the initial amount of trust according to the outcome of the authentication of the partner. To establish trust in a MANET of mobile phones without preshared data or central instances devices can start with a minimal amount of trust and can earn more by behaving correctly. In a different approach, initial trust is derived from social data locally available on the phone.

2.2.1 Trust by Authentication

Commonly, in computer networks a trustworthy communication is established through authentication. It is used to assure the identity of the communication partner or his membership to a known group. Based on this information a level of trust can be derived. Existing authentication methods require either a shared secret or a central instance for verification. While providing pairwise shared secrets between all mobile phones is an unrealistic deployment scenario, a central instance needs to be accessible at all times. Both contradicts the paradigm of ad hoc networks. In addition, in a scenario, where a phone's Internet connection is interrupted or unsafe only locally available information can be used for authentication.

2.2.2 Earning Trust by Reputation

In a reputation-based system, nodes of a network exchange reputations of other nodes and derive a personal trust value based on this. Nodes initially start with a minimal amount of reputation and earn positive reputation over time, if no malicious behavior is noticed by dedicated observers. Monitoring can be done by checking the content of a relayed message using a different path [7] or by observing the radio activity of a node and thus noticing packet alterations, drops, or replays [8, 9, 10]. By interchanging reputation information between the nodes the network converges and malicious nodes get known and eventually isolated in the network.

A major disadvantage of using positive reputation acquired over time is the intention hiding problem: An attacker behaves honestly for some time and thus earns good reputation, which he can eventually use to potentially do even bigger harm by exploiting the trust acquired by its peers. An additional problem arises from inherent characteristics of wireless communication. Common metrics such as packet loss to identify malicious behaviour interfere with an accurate rating of devices. Since messages may not be correctly received by a phone due to reflections, noise etc. false accusations will be made. The exchange of reputations is furthermore not suited for spontaneous and short-living MANETs because earning trust and its convergence in the network depend on time. To achieve reliable results a network needs a sufficient dense population. It should be possible that every node is evaluated by more than one other node, in order to generate a balanced view of its behavior.

2.2.3 Establish Trust by Social Data

To decide quickly about another phone's trustworthiness, a system is needed, where an initial trust can be determined in a short time. Conventional, technical authentication methods do not work when meeting an unknown device, where a central instance is generally not available. Since each mobile phone is associated with a user, trust between phones can be defined not only technically but also based on social data. If two people trust each other, it is unlikely that one of them will prepare his phone in a way that would harm the data integrity or privacy of the other party.

Personal information that is inherently available on a mobile phone, can be a fundamental source to examine the user's relationship to other people. Contacts can be stored with telephone numbers, email addresses, and OSN information. Each of those three data types can help to identify a person. Using this information, phones get to know the immediate social networks of their users. Since not all contacts are equally important to a phone owner, information about the amount and frequency of communication can be used to assign a quality to each contact. A high number of telephone calls, messages, or emails with a contact show a high degree of communication and closeness.

Finding phones of friends, i.e., trusted individuals, or of

friends of friends, can be an approach to solve the trust problem in mobile phone MANETs. In comparison with strangers' phones that do not have any incentives to be of assistance, helping a friend, or even a friend's friend, can be a legitimate reason to spend more computational and energy resources.

2.3 Open Challenges

Using conventional, technical authentication, it is hard to identify an unknown mobile, without access to a central database. With the help of the inherent social information on the phone, this task is easier and in addition provides incentives to let another phone relay data via your device.

As soon as a friend or a friend of a friend has been identified, a trust relationship can be assumed. But not every entry in a contact list is a trusted friend. Even when the amount of communication is consulted as a metric, frequent interactions could also be an indication of an ongoing conflict. If a longer period of time is observed, however, numerous interactions denote more likely a close relationship [11]. When using such a system in a business context, contacts in a mobile phone are generally not close friends and on the contrary might be competitors that should not be trusted. On the other hand, there is always a high security risk, when sending sensible company information over a multi-hop MANET, regardless of the means of authentication involved.

While it is improbable that a trusted friend tries to attack one's data's integrity or privacy, his phone may be compromised clandestinely by malware. This scenario can not even be prevented by cryptographic, technical authentication.

3. CONCEPT

The social network of an individual is reflected on his phone through his contacts and communication flows. Based on this information, phones can try to identify phones of acquaintances and friends to establish a trust relationship.

3.1 Background: Using Mutual Entries

Two phones that interact locally can determine the level of familiarity of their users by comparing their contact lists. A mutual contact is found if at least one of the entries such as telephone numbers, email addresses, or OSN IDs is mutual. Reciprocal entries can indicate the corresponding contact to be a mutual acquaintance or friend. Conclusions can be derived from the number of shared contacts and entries as well as the closeness of the user to the corresponding contacts.

3.1.1 Quantity of Mutual Contacts

The number of mutual contacts can be an indication for the closeness of two users [1]. It can give an idea if the two users associate with the same people. If two users share a number of mutual contacts, it is likely that they share a common group of friends or have even exchanged contact information themselves, thus increasing the trust between the users. The obvious attack possibility, where the attacker just claims a whole phone book to be his contact list, can be avoided, if the number of entries serving as input to the comparison is limited to a standard contact list's size.

3.1.2 Tie Strength

Evaluating the closeness of a mutual contact to a user allows this user to assign a quality to this mutual contact. This evaluation is done by means of tie strength, a measure for relationships [1]. So-called weak ties reflect acquaintances, whereas strong ties refer to trusted friends and family. To range the contacts of a user between those two extremes, they are evaluated using the type of entries as well as duration, intensity, and intimacy of the relationship to the contact [11].

Becoming someone's OSN friend is generally an effortless procedure and does not even require message exchange between the users. Adding a phone number or email address to the own contact list is usually done more consciously or, if done automatically, after initial contact has taken place, i.e., through a call or an email. Thus, a contact that is associated only to an OSN ID can be considered a weaker tie than one with telephone numbers or email addresses, respectively.

A long lasting relationship is an indication of a stronger tie and the date of the first interaction with a contact may indicate the duration of a relationship. However, the creation time of the contact list entry or the OSN association cannot be determined on mobile phones in many cases. Further indicators of strong ties are the intensity and intimacy of a relationship, which can be derived from the interaction frequency and the refresh period of communication, respectively [11]. The aggregated duration of calls can be a substitute for tie strength as well [12]. All of those parameters can be obtained from the analysis of past communication activity. Call lists, email conversations, and messages or posts exchanged in OSNs give information about the frequency and length as well as the time of the first and last interaction.

Strong ties within the mutual contacts can enhance the level of trust towards the other user. Equally important is, however, the strength of the other user's tie with the mutual contact. With the analysis of the mutual entries of a mutual contact, this tie strength can be estimated. If a user has, for example, a full set of phone number, email address, and OSN ID of a mutual contact, but the only mutual entry is this last ID, it can be concluded that the other user's tie to that contact is not as strong. On the other hand, if both users share several different phone numbers or email addresses of one contact, they both appear to be strong ties to that contact, which can enhance their mutual trust.

3.2 Technical Realization

In order to find mutual trusted contacts with another phone, contact list entries have to be compared between two phones. However, not all entries in a contact list represent individuals. Common business contacts, such as nationwide hotlines or the email address of a local supplier, are listed in the address book of many users but in general do not represent a personal relationship. Typically, they are not related to a specific individual and if they are, merely represent the business side of an interpersonal relationship. Therefore they should not be considered when looking for mutual contacts. To achieve this, we tag the entries by adjusting the local address book with business registers like yellow pages. This can be done by the mobile phone on a regular basis, when the phone is charging and a reliable link is available, for example. Special numbers (e.g., toll-free hotlines) can be eliminated in advance by means of their explicit prefix.

To assure that different syntax of numbers or email addresses do not prevent a successful comparison, those entries have to be normalized. In phone numbers all non-numeric characters are excluded. To further avoid international prefixes or country codes, only the last 8 digits are considered. This is reasonable since in mobile phones area codes should be included in the phone number to guarantee global reachability. More than 8 digits can lead to conflicts with countries not using the 3+7 digit system, e.g., Germany. Email addresses should be inspected in terms of the convenience function the email providers allow. For example, Google's email service Gmail permits the users to insert dots between any two characters of its addresses and still smoothly delivers the mail to the original account. Also a "+" with arbitrary text can be added at the end of the local part of the address. Considering these policies, different notations of email addresses can be normalized.

To actually find mutualities with a neighboring phone, a mobile may distribute all contact list entries using Bluetooth or other near-field communication technologies. However, privacy concerns prohibit this approach. The entries need to be encrypted in a way that the mutual contacts are only visible to the negotiation partner, while an eavesdropper on the wireless medium cannot gain any information about actual contacts. The use of a commutative encryption scheme can securely solve the two party set intersection problem [13].

Arb et al. [14] introduce a straightforward protocol for mobile phones, where all numbers in a phone's contact list are negotiated using commutative encryption. When two phones A and B meet, phone A encrypts every entry e in its contact list with a secret random key α and sends the resulting list of e_α to B. Phone B replies with its own randomly encrypted list of contact list entries e_β. Additionally, B encrypts the entries it received from A with its own key and transmits the resulting $e_{\alpha\beta}$ as well. Phone A analogously sends $e_{\beta\alpha}$. Because of the commutative nature of the encryption function, $e_{\alpha\beta} = e_{\beta\alpha}$ for equal entries e. This way the phones find out mutual telephone number entries without revealing any other contact information.

Extending this technique to other entry types of the contact list, which uniquely identify an individual, such as email addresses and OSN IDs, this method can be used to find mutual contact list entries between two phones. The outcome can be applied to characterize well-disposed neighbors.

4. MEASUREMENT-BASED ANALYSIS

In this section, we present a preliminary evaluation of our sociologically-inspired approach to establish trust between two mobiles. The intention of the analysis is to gain a first estimator of the contact lists characteristics. Based on real-world data this helps to roughly identify potentials and limitations of our concept.

4.1 Evaluation Setup

We collected a small number of contact lists from heterogeneous groups (i.e., family, friends, and colleagues), retrieved from Android or iOS devices – containing telephone numbers as well as email addresses. Information about OSNs was not widely available in the sample group and therefore not considered in this evaluation. It is hard to convince people to record their communication patterns. In the current state, we thus conduct only a quantitative analysis that excludes tie strengths. For each contact list pair, we calculate the number of mutual contacts. For every match, we differentiate per contact type, i.e., if just a telephone number, an email address, or both entries are mutually present. In total we analyzed 12 contact lists with numbers of entries that range from 45 to 495.

4.2 Results

The subjects providing contact lists could be socially classified into four groups. Within one group, the subjects were well acquainted with each other. However, members of one group hardly knew members of the other group. This topology is also reflected in the number of mutualities of their contact lists. While one subject shared as much as 24% of his contacts (or 20 entries) with another member of the same group, the highest number of mutual contacts between subjects of different groups were 2 (2.4% of the contacts). The total number of mutual contacts within one group ranged from 4 to 28, whereby a high percentage of this contacts had more than one mutual entry, e.g., a mutual telephone number as well as an email address.

Despite the low number of contact lists in this analysis, it is clearly visible that the list size is quite heterogeneous and varies by one order of magnitude. While some individuals are eager collectors of addresses and telephone numbers, others select very carefully who will be included in the list. Thus, a very low number of mutual contacts cannot be used to justify a trust relationship, since a trust relationship between a user and every one of his contacts cannot be expected in general. Furthermore, the relative number of mutual entries varies as well. For example, one pair of subjects in the analysis had 20 mutual contacts, which accounted for 24.3% of the contacts of one of the subjects, but it represented only 4.7% of the contacts of the other subject.

These significant differences in the user behaviour regarding the own contact list show that an exclusive analysis of the quantity of mutual entries is insufficient. A personal weighting based on tie strength for every mutual contact list entry can help to generate a more pronounced trust evaluation. However, the user's behavior will also affect the data observed to calculate tie strengths, e.g., the number of transmitted messages may vary substantially. Still, a classification of the contacts can be given due to relative communication patterns. A highly communicative user, writing twice a day to a friend, may find this relationship just as strong, as a user who writes less in general and communicates only once a week with his friend. The examination of *relative* activity can mitigate the varying user habits.

The transmission of the complete contact list constitutes a notable amount of data traffic. With 240 contacts per contact list, the average in the test setup, and 3 entries per contact, e.g., phone number, email address, and OSN ID, the data volume is more than 11 kB if an 128 bit hash function is used. With the first Bluetooth generation, this transmission would take about 1 second. Thus it should be assured, that the evaluation of a neighboring phone is conducted only when necessary.

5. DISCUSSION & RESEARCH AGENDA

While the method described in Section 4 provides an autonomous and lightweight way to evaluate trust between two phones, there are still a number of questions, which we address in the following section.

5.1 Discussion

Intense communication is not a good indicator for closeness—On the one hand, a high degree of correspondence (i.e., message exchange or frequent phone calls) shows an ongoing social relationship [15]. On the other hand, this communication pattern may also rather imply a dispute than a close and amicable tie. However, Gilbert et al. [11] show that frequent interaction over a longer period of time more likely denotes a close relationship. Thus, the evaluation of tie strength needs to consider not only recent activities but comprise long-term observations.

The device of a friend is compromised—On the basis of analyzing mutual contacts a mobile phone can identify phones of individuals, who can be trusted to some degree. Despite the well meaning owner, its phone can be compromised and thus contradicts trust. Such a conflict occurs if the other device is (a) infected by malware or (b) the phone was stolen. Both cases address a problem, which is also present in the context of other device-oriented authentication mechanisms. It is worth noting that our approach does not promise to guarantee a 100% trust but provides ad hoc techniques to estimate trust. Knowing the identity of the owner (or primary user) does not protect against unknown or intentional attacks of the current user. This fact has to be considered when assigning trust to the communication party. Contacts could be grouped locally by the risk to be infected by malware or let it get stolen. If the majority of mutual contacts belong to the same group, the trust values could be assigned accordingly. Thus, the risk can be decreased but it demands manual effort in the clustering process. More importantly, we argue that there is an intrinsic interest of the owner of the phone to secure his personal data against (sofware- or hardware-based) theft. The system itself should be protected by anti-virus programs and sensitive information should be available locally only if the user has been authenticated, e.g., via PIN code or OSN passwords.

Users may not want their data relayed by people who know them—A node relaying packets is able to intercept personal information, if no encryption is used, or to create a traffic profile. While generally in a network it is not trivial to associate an IP address at a specific time with a certain individual, usually, mobiles are permanently assigned to its users. However, our concept does not intend to expose the specific identity of a person. It identifies friends. People who do not want that data will be relayed by friends may apply our concept in a vice versa direction. Users can still dynamically decide if they establish an ad hoc communication. On the other hand, privacy can be preserved by IPsec tunneling.

The users learn about the reciprocal selection of contacts—Based on the scheme described in this paper, the users learn about the identity of their mutual contacts. There is a simple adjustment to the algorithm that prevents this. If at least one party randomizes the order of the twice encrypted contacts before sending them back, only the number of mutual contacts can be calculated. While this provides a very privacy conscious mechanism, it derogates the potentials of the trust analysis, since no tie strength ratings can be performed. To avoid the revelation of sensible contacts and still allow for tie strength evaluations, users could mark the specific entries to be excluded from the contact list comparison.

An attacker can gather social information in advance—One risk emerging through the use of contact information to assign trust is that contact list entries become more valuable. Attackers can aim to collect publicly available IDs of friends in OSNs as well as email addresses and phone numbers of a user's environment. This information can lead to targeted phishing attacks and can be used to gain trust. Corresponding attacks are not novel. Gaining social trust in an OSN by becoming friends with friends of the victim, has already been described [16]. The awareness for this kind of criminal activity should be strengthened both in the public opinion, as well as in the OSN context. A phone book attack (cf., Section 3.1.1), in which the attacker just claims a big number of contacts, e.g., from publicly available sources, to be in his contact list can be met by restricting the number of contacts to compare.

Not all mutual contact entries can be revealed—Due to the diversity of phone numbers and email addresses every individual has today, it is quite challenging to reveal all mutual contacts, even of close friends. In the current state, our proposal does not include merging of different IDs that belong to the same individual. It is an open question if this is possible at all in a distributed way. Consequently, our concept produces false negatives. This leads to trust evaluations that are slightly less optimistic than they could be. It should be noted, however, that while this fact results in less trust, our approach does not produce false positives, i.e., it does not assign more trust to another subject than it can be supported by the data available. This inaccuracy does not lead to inappropriate suggestions in terms of security.

5.2 Research Agenda

To explore the potentials of socio-inspired trust establishment in general, it is fundamental to analyze the application of sociological insights into the technical context in more detail. We believe that smartphones are a good starting point as they inherently provide a rich set of social data and require ad hoc trust establishment. They bridge the gap between the traditional (telephone) and current (online social network) paradigm of distant interaction between people.

In his seminal work [1], Granovetter deals only with strong, weak, and absent ties between individuals. In order to compare relationships more flexible, a granular scale is needed. Later studies (e.g., [17]) introduce tie strengths not only based on an absolute scale, but also on a relative. In the context of socio-inspired security, it is especially important to know if and how exactly social relationships can be quantified. Will it be necessary and possible to absolutely define a scale for tie strength or will it be sufficient to use it as a measure of comparison between two or more subjects? Furthermore, how accurately can such an absolute or relative scale represent real-life relationships? It is also necessary to evaluate lower and especially upper limits of tie strength that constrain a meaningful analysis of trust.

Tie strength has yet been derived from many different observable phenomena, e.g., local closeness [17], email traffic [15], and phone usage [18]. As described in Section 3, we believe that call logs as well as the history of email traffic and OSN messaging can be a valid foundation to evaluate tie strength. The interaction of all data available on a mobile phone, however, has to our knowledge not yet been used to evaluate tie strengths. Moreover, due to the constantly growing amount of data available in OSNs, e.g., information about family members, new data sources need to be evaluated.

In order to gain information about the tie strength of a

party in a contact list, recent communication logs are examined. The analysis of call registers covering a whole year, for example, can give an accurate picture of the intensity of communication to a specific contact. The examination of calls to this individual during the last hour, however, does not carry much information about the social relationship. Extending the examination period to 24 hours or even a week might not deliver significant results. Furthermore, a longer observation period produces more accuracy in terms of the nature of the relationship [11], e.g., to rule out an ongoing dispute. Therefore, the trade-off between observation period and accuracy of the results should be investigated. What minimum time window needs to be observed in order to obtain reliable output? Furthermore, the storage of long term call logs and email traffic patterns may take up a substantial amount of memory space and thus requires efficient storage at resource limited mobiles.

Since features once unique to phones, e.g., making calls, today are easily executed with a PC at home, the analysis of tie strength might not be limited to be used solely with smartphones. Pursuing the idea of integrating all kinds of social interactions as input to evaluate tie strength may entail interesting new features in the context of security and privacy as well as specific applications such as OSNs. Automatically, new friends could be suggested or groups of close friends could be created and maintained. This could lead to an improved privacy, as the user could easily decide to share certain information only with his closest peers.

6. CONCLUSION

The information held in contact lists and conversation logs on mobile phones can be very useful to define relationships to other phones. The numbers of mutual contacts can roughly indicate a trust relation between two devices. Taking the concept of tie strength into account, a more sophisticated view can be generated. The contribution of this paper is not only the idea of comparing contact lists to derive trust between two mobiles, but to integrate and combine further social vetors, which leads to socio-inspired trust and security.

In this paper, we presented a detailed discussion about trust establishment between mobiles and analyzed preliminary measurement results for our lightweight, ad hoc scheme. Through sociological analysis we showed that trust between two individuals can be estimated using only technically observable local data. Our future work on autonomous trust establishment will follow the introduced research agenda. In a first step, we will extend the current study and focus on evaluating the tie strength of a phone's user with the entries in his contact list. We will also analyze data of totally unrelated people. A detailed evaluation of tie strength can lead to new insights regarding the trust between two mobile phones' users and, thus, the level of trust between two phones.

7. REFERENCES

[1] M. S. Granovetter, "The Strength of Weak Ties," *The American Journal of Sociology*, vol. 78, no. 6, pp. 1360–1380, 1973.

[2] L. A. Renzulli and H. Aldrich, "Who Can You Turn To? Tie Activation within Core Business Discussion Networks," *Social Forces*, vol. 84, no. 1, pp. 323–341, 2005.

[3] D. G. Murray, E. Yoneki, J. Crowcroft, and S. Hand, "The Case for Crowd Computing," in *Proc. of the 2nd ACM SIGCOMM MobiHeld Workshop*. New York, NY, USA: ACM, 2010, pp. 39–44.

[4] H. Falaki, D. Lymberopoulos, R. Mahajan, S. Kandula, and D. Estrin, "A First Look at Traffic on Smartphones," in *Proc. of the 10th IMC*. New York, NY, USA: ACM, 2010, pp. 281–287.

[5] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, "Architectural Guidelines for Multipath TCP Development," IETF, RFC 6182, March 2011.

[6] S. Barré, O. Bonaventure, C. Raiciu, and M. Handley, "Experimenting with Multipath TCP," in *Proc. of the ACM SIGCOMM 2010 Conference*. New York, NY, USA: ACM, 2010, pp. 443–444.

[7] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "Faces: Friend-based ad hoc routing using challenges to establish security in manets systems," *Systems Journal, IEEE*, vol. 5, no. 2, pp. 176–188, 2010.

[8] W. Li, J. Parker, and A. Joshi, "Security through Collaboration in MANETs," in *Collaborative Computing: Networking, Applications and Worksharing*, ser. Lecture Notes of ICST. Springer Berlin Heidelberg, 2009, vol. 10, pp. 696–714.

[9] Z. Zhang, P.-H. Ho, and F. Naït-Abdesselam, "Radar: A reputation-driven anomaly detection system for wireless mesh networks," *Wirel. Netw.*, vol. 16, no. 8, pp. 2221–2236, November 2010.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. of the 6th ACM MobiCom*, New York, NY, USA, ACM, 2000, pp. 255–265.

[11] E. Gilbert and K. Karahalios, "Predicting tie strength with social media," in *Proc. of the 27th ACM CHI Conference*. New York, ACM, 2009, pp. 211–220.

[12] J. Banford, A. McDiarmid, and J. Irvine, "Estimating the Strength of Ties in Communication Networks with a Small Number of Users," *6th Intl. Conf on Wireless and Mobile Communications*, pp. 191–195, 2010.

[13] B. A. Huberman, M. Franklin, and T. Hogg, "Enhancing privacy and trust in electronic communities," in *Proc. of the 1st ACM Conf. on Electronic Commerce*, ACM, 1999, pp. 78–86.

[14] M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "Veneta: Serverless friend-of-friend detection in mobile social networking," in *IEEE Intl. Conf. on Wireless and Mobile Computing*, October 2008, pp. 184 –189.

[15] G. Kossinets and D. J. Watts, "Empirical analysis of an evolving social network," *Science*, vol. 311, no. 5757, pp. 88–90, January 2006.

[16] R. Potharaju, B. Carbunar, and C. Nita-Rotaru, "iFriendU: Leveraging 3-cliques to enhance infiltration attacks in online social networks," in *Proc. of the 17th ACM CCS*. New York: ACM, 2010, pp. 723–725.

[17] N. Eagle, A. S. Pentland, and D. Lazer, "Inferring friendship network structure by using mobile phone data," *Proc. of the National Academy of Sciences*, vol. 106, no. 36, 2009.

[18] N. K. Baym, Y. B. Zhang, and M. C. Lin, "Social interactions across media," *New Media & Society*, vol. 6, no. 3, pp. 299–318, June 2004.