On the Tradeoff between Trust and Privacy in Wireless Ad Hoc Networks

Maxim Raya, Reza Shokri, Jean-Pierre Hubaux

School of Computer and Communication Sciences, EPFL, Switzerland
{maxim.raya, reza.shokri, jean-pierre.hubaux}@epfl.ch

ABSTRACT

As privacy moves to the center of attention in networked systems, and the need for trust remains a necessity, an important question arises: How do we reconcile the two seemingly contradicting requirements? In this paper, we show that the notion of data-centric trust can considerably alleviate the tension, although at the cost of pooling contributions from several entities. Hence, assuming an environment of privacy-preserving entities, we provide and analyze a game-theoretic model of the trust-privacy tradeoff. The results prove that the use of incentives allows for building trust while keeping the privacy loss minimal. To illustrate our analysis, we describe how the trust-privacy tradeoff can be optimized for the revocation of misbehaving nodes in an ad hoc network.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection (e.g., firewalls)*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Economics, Security, Theory

Keywords

Game theory, Privacy, Trust

1. INTRODUCTION

Security and privacy are often said to be at odds. Much of this tension boils down to the cost of establishing the trustworthiness of entities (e.g., network nodes), which requires them to disclose their private information. Typical solutions to this problem propose trading privacy for trust [14], i.e., gradually revealing an entity's private information to gain a sufficient level of trust. But the majority of these works address e-commerce environments where, rightfully, the emphasis is on establishing the trustworthiness of individual entities. Yet, with the emergence of collective intelligence where only the opinion of a group matters, the data is becoming more important than its sources. In addition to special instances of online environments (e.g., Wikipedia), certain types of wireless networks are actually data-centric by nature. For example, users of sensor networks require the sensed data to be correct while completely abstracting the sensing platform, i.e., the individual sensor nodes. Another example is ephemeral networks, such as vehicular networks, where encounters among nodes are often short-lived. Building entity-centric trust in such cases would be an overkill, if not impossible altogether. This naturally calls for establishing the trustworthiness of the data itself.

In a nutshell, data-centric trust is built by collecting all the evidence corroborating a piece of information [11]. Intuitively, the more entities that corroborate the information, the higher the resulting trust value is. This has a valuable side effect if the required trust level is a threshold that is independent of the number of participants: The individual contributions of entities decrease as the number of entities increases and hence the amount of privacy that needs to be traded for trust also decreases. But this improvement in privacy comes at a cost when privacy-preserving entities have to collectively contribute to the establishment of data-centric trust in the presence of adversaries. In fact, a privacy-preserving entity is *rational* by definition, from the privacy point of view. This is because it optimizes its own utility (actually, it minimizes its privacy loss) and hence prefers contributing nothing to the system while getting all the benefits, thus creating the free rider problem [4]. To address this issue, we use game theory to model the strategies of rational entities that try to establish data-centric trust in the presence of rational adversaries. Based on the initial analysis, we prove that using incentives can enable trust establishment and reduce the amount of disclosed privacy.

To illustrate the above problem, let us consider an example scenario based on an important security primitive - the revocation of credentials of misbehaving nodes. Whereas in a system architecture with an online Certificate Authority (CA), the latter takes care of revoking credentials, the intermittent availability of the CA in wireless ad hoc networks calls for alternative solutions. A popular solution is the use of a voting scheme whereby a set of nodes have to contribute their individual votes to revoke a misbehaving node [9]. These works assume that nodes vote by default. But as voting consists in sending private information, such as credentials and location information, it is reasonable to expect privacy-preserving (and hence rational) nodes to

WiSec'10, March 22–24, 2010, Hoboken, New Jersey, USA.

free-ride on the contributions of other voters. Consequently, voters face a tradeoff between contributing to the collective vote, that is essentially the trust level in the revocation decision, and preserving private information (especially real-time location) that can be lost by casting a vote.

By addressing the trust-privacy tradeoff in a rational environment, we believe that this paper constitutes one of the first steps towards studying privacy systems with "human" properties (e.g., rationality), a necessary research area as computers increasingly reflect the preferences of their owners. We assume that users will try to rationally protect their privacy, i.e., reveal only the minimum amount of private information required to benefit from certain services (e.g., location-based search). Obviously, people are not completely rational, but a properly configured software agent will be able to better enforce the rational preferences of its operator. For example, the Platform for Privacy Preferences (P3P) Project [1] translates user privacy preferences to software agents. Moreover, the recent success of startups that use incentives to motivate users to reveal their locations and contribute reviews confirms the assumption of rational participants.[1] Thus, our work is the extension to privacy of the works bridging cryptography and game theory [7], and notably rational multiparty computation [5].

This paper is organized as follows. Section 2 discusses the related work. Section 3 describes the system and threat models. Section 4 analyzes, using game theory, the tradeoff problem. Section 5 concludes the paper.

2. RELATED WORK

Seigneur and Jensen [14] propose an approach to achieve the tradeoff between trust and privacy in online transactions where entities use pseudonyms. To preserve privacy, entities use different pseudonyms for different transactions, thus preventing the linkability of these transactions; a reputation level is attributed to each of these pseudonyms. But to increase the level of trust in an entity, the latter has to link several pseudonyms, thus combining the corresponding reputation levels. The number of pseudonyms to link depends on the required trust level. Seamons et al. [13] describe several solutions to the disclosure of private information during trust negotiation between two entities, namely a client and a server on the Internet. Yao et al. [15] formalize a point-based trust management model that allows revealing the least sensitive private information (with the least attributed points), as long as the sum of points satisfies the threshold for gaining access to the server resources. Lilien and Bhargava [8] discuss the conflict between privacy preservation and trust establishment in online interactions. They assume that users have a set of private attributes that they want to conceal and a set of corresponding credentials that are helpful in establishing trust in these users. The tradeoff problem is formulated as the choice of the minimum number of credentials to be revealed for satisfying trust requirements, such that the users' privacy loss is minimized.

Online reputation systems, where users report the quality of products, pose problems essentially of data-centric trust. Jurca and Faltings [6] analyze incentive mechanisms for honest reporting in these systems and propose payment schemes that rely on the correlation among the reports of different reporters. Acquisti et al. address the use of incentives for providing and using anonymity services [2].

Last but not least, there is a close similarity between our problem and rational multiparty computation (MPC) in cryptography [5]. Rational MPC can potentially solve the trust-privacy games, but it incurs, due to its generality, several modeling and efficiency constraints (general MPC protocols typically require interactive computations, such as the distribution and combination of secret shares). By creating a customized model, we avoid these complications and provide an efficient solution.

3. SYSTEM AND THREAT MODEL

We assume a wireless network where communication among entities (i.e., network nodes) is locally broadcast and each entity is able to receive an ongoing broadcast before sending a new message, i.e., communication is *sequential*. We also assume that there are deadlines on making decisions and model this by making communications right before the deadline simultaneous and not sequential, implying that collisions may happen and some messages may not be received by the deadline. Entities are computationally powerful and are capable of using public-key cryptography. Hence, we assume that messages are digitally signed and their senders can be anonymously authenticated, e.g., using anonymous public keys with valid credentials issued by a Certificate Authority (CA). All entities are distinguishable, i.e., they have different identifiers. If an entity has several legitimate identities, such as pseudonyms, we consider them as different entities. This means that the CA is responsible for preventing the abuse of multiple identities. One way to achieve this is to issue identities with non-overlapping validity periods and make the obtention of new identities costly. In addition to credentials, entities communicate other attributes, such as their location. We assume that entities cannot lie about these attributes without being detected. More specifically, we assume that positioning (e.g., GPS) and secure location verification systems [12] are in place, thus preventing nodes from reporting false locations; the fulfillment of this assumption is out of the scope of this paper, given the rich existing literature on the subject. Last but not least, we assume that entities are privacy-preserving (i.e., they are rational from the privacy point of view) and hence minimize their privacy losses (i.e., they optimize their own utilities).

The goal of the system is to disseminate truthful information. Entities are divided into two groups: benign and adversarial. Adversaries have the same properties as benign nodes, but disseminate false information. This can be due to an intended attack or merely a fault in an entity's information acquisition or generation systems. Adversaries can also disseminate the same false information to increase its trustworthiness. Entities reveal their attributes (e.g., credentials, precision of location, etc.) to increase the trust level of the information they disseminate. But by revealing these attributes, entities also reduce their privacy. The example information dissemination system that we use in this paper is a revocation system where nodes locally broadcast votes against misbehaving nodes. Once a given vote threshold (e.g., a fixed number of votes) is reached, the misbehaving node is revoked by its neighbors. We will not go into further details of the revocation system as this is a well covered subject in the literature [9, 16]. In the revocation

[1]For example, by rewarding participants who check-in at their favorite locations, the *foursquare* service has developed a large user base much faster than its predecessors that were based solely on non-remunerated contributions [3].

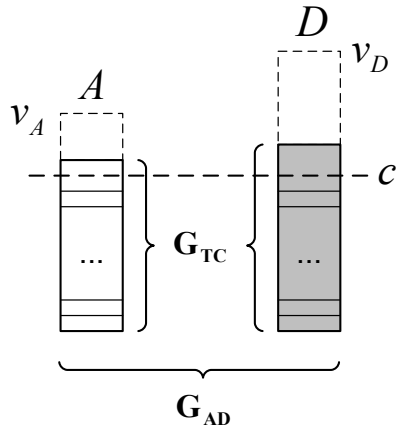

Figure 1: The duality between the trust-privacy games. $\mathbf{G_{AD}}$ is between the two groups A and D, whereas $\mathbf{G_{TC}}$ determines how microplayers in each group contribute to $\mathbf{G_{AD}}$. The winner of $\mathbf{G_{AD}}$ is indicated by the shaded rectangle (note that D reaches a higher level of trust, by revealing more private information, than A). The dotted rectangles represent the gains v_A and v_D of the macroplayers in the case of winning the game. c is the minimum amount of privacy required to reach the threshold trust θ.

example, the goal is to achieve a sufficient trust level (e.g., the vote threshold) in the revocation information. We assume that an information verifier V, which can be any node, needs to make a revocation decision based on the votes it receives from the neighbors of a misbehaving node. Let θ be the threshold trust level that the information verifier requires to accept a piece of information.

In our model, we do not address the leakage of private information by mechanisms other than the trust establishment mechanism. For example, individual entities may reveal their network-layer identifiers, such as IP addresses, when sending information. Although this constitutes a privacy loss, it is orthogonal to our model. In fact, we model only the loss of information that entities cannot conceal (they need to provide evidence), whereas network-layer identifiers can be anonymized.

4. TRUST-PRIVACY GAMES

By definition, privacy-preserving entities try to minimize the loss of their private information, which implies that they behave *rationally* (i.e., they try to optimize a given utility function) from the privacy point of view. And given that private information is traded for trust, rational entities make data-centric trust establishment difficult because it has to compromise conflicting requirements: Privacy-preserving entities have to contribute a sufficient level of trust without unnecessarily revealing too much private information. This optimal level is obviously the threshold trust level in the absence of an adversary, but when an adversary tries to surpass the benign entities, the latter have to enter a competition with the adversary while trying to minimize the attributes they reveal. In addition, as different combinations of entities (from the total set of K) can reach the threshold trust level, with each entity contributing an adjustable amount of its private attributes, it becomes paramount to find and implement a mechanism that makes the individual contributions both sufficient and fair. It is even questionable whether the entities would contribute at all to trust establishment.

The above questions naturally call for the use of game theory to solve two related games: the *Attacker-Defender Game* $\mathbf{G_{AD}}$ and the *Trust Contribution Game* $\mathbf{G_{TC}}$. $\mathbf{G_{AD}}$ captures the competition between attackers and defenders to support their respective versions of the truth. In the revocation example, the defenders would vote for revoking a misbehaving node whereas the attackers would vote for keeping this node in the system.[2] $\mathbf{G_{TC}}$ models the details of $\mathbf{G_{AD}}$ by defining the individual amounts of privacy to be contributed by benign entities to collectively win $\mathbf{G_{AD}}$. Put differently, $\mathbf{G_{AD}}$ is on the macroscopic level where the attacker and the defender represent the sets of adversarial and benign entities, respectively. $\mathbf{G_{TC}}$ analyzes at the microscopic level how benign entities behave individually to collect the defender's trust level in $\mathbf{G_{AD}}$. Figure 1 illustrates this duality. We refer to players in $\mathbf{G_{AD}}$ as *macroplayers* and to players in $\mathbf{G_{TC}}$ as *microplayers*.

4.1 Game-Theoretic Model

To model the trust-privacy games, we need to make some assumptions about the way the macroplayers interact (Section 3 describes the model for microplayers). First, we assume that the information verifier needs to make a decision by a given deadline (e.g., it needs to decide based on the revocation votes that it receives whether to trust the next message from the misbehaving node). Second, we assume that macroplayers can observe, before acting, the actions of preceding macroplayers in all but the last stage of the game (cf. Section 3). In this last stage, just before the deadline, both macroplayers try to act in order to win the game and are thus unaware of the actions of the other macroplayer. As the action of only one macroplayer will be retained in the last stage, we need to assign the probabilities of winning to each macroplayer. The resulting game is called *dynamic Bayesian game* where "dynamic" means that the game is sequential and "Bayesian" refers to the probabilistic nature of the game. Dynamic games are represented by a tree where the players occupy the nodes of the tree and their actions are the branches descending from the respective nodes. Last but not least, we assume that macroplayers have enough privacy to trade for trust. This assumption is reasonable in an environment where new entities can appear, thus increasing the available privacy resources. The information verifier has two options of action when receiving information with an insufficient trust level. The first option is to take the information with the highest, though insufficient, trust level. The second option, if time permits, is to broadcast a request for new evidence, thus restarting the trust games.

The solution concept for dynamic Bayesian games is called *Perfect Bayesian Equilibrium* (PBE) and can be computed by finding the *best response* of each player, i.e., the set of actions that maximize the player's utility given the actions of the other players. We will not go into further conceptual details here but refer the interested reader to [4].

[2]Obviously, the attackers in this case are not directly identified as misbehaving. The terms "defender" and "attacker" merely refer to opposing sides in the game.

4.2 Attacker-Defender Game

In $\mathbf{G_{AD}}$, both the attacker and the defender try to prove to the information verifier their respective versions of the truth. It is worth reiterating here that the two macroplayers (attacker and defender) actually represent the groups of adversarial and benign nodes, respectively, on the macroscopic level. The winner is the macroplayer that succeeds in providing the higher trust level before the game deadline. As the game is dynamic, each macroplayer has the possibility to play more than once, each time surpassing the other macroplayer's previous action. As the attributes needed to increase the trust level also diminish a macroplayer's privacy, each macroplayer should try to reveal as few attributes as possible in surpassing the other macroplayer.

Figure 2 illustrates $\mathbf{G_{AD}}$. The two macroplayers are A (attacker) and D (defender) with two possible actions: S (send attributes to the information verifier V) and W (wait until the next stage). When sending, each macroplayer increases the level of trust in its information but the opponent can surpass it in the next stage, thus requiring the first macroplayer to disclose even more attributes in the subsequent stage.[3] By waiting, a macroplayer has a probability (p_A for A and p_D for D) of winning the game without the escalation of attribute investment. The winner has to provide a trust level at least equal to a defined threshold, θ as defined in Section 3. Let c be the privacy loss required to reach θ. Hence, each macroplayer is required to invest at least an amount c of privacy to win the game. Let δ be the minimum increment required to surpass the previous action. Last but not least, let v_A and v_D be the gains of macroplayers A and D, respectively, when winning the game. v_A represents how much the attacker benefits from a successful attack, whereas v_D represents the cost that the defender avoids by preventing the attack.

In practice, p_A and p_D depend on the individual entities that compose A and D. For example, in an IEEE 802.11 wireless network, if all entities have the same access probability, p_A and p_D are the fractions of entities in A and D, respectively, out of the total number of entities. Learning p_A and p_D before the game is hard, but we will show that it is actually possible to achieve the desired outcome by selecting configurable parameter values independently of these two probabilities. Hence, our model does not require the knowledge of p_A and p_D.

4.2.1 Equilibrium

By solving $\mathbf{G_{AD}}$, we can find its equilibrium, i.e., the set of player strategies from which none of the macroplayers can unilaterally deviate while realizing a better payoff. We assume that the defender plays first, as it has to establish trust in the information it provides and may not be aware of the attacker (this is its typical behavior when no attacker is present). In the following solution of $\mathbf{G_{AD}}$, the tuple (σ_D,σ_A) contains the strategies of D and A, respectively.

THEOREM 4.1. *The strategy* (W, WW) *is a PBE of* $\mathbf{G_{AD}}$.

This means that D's best strategy is to play always W and A's best-response strategy is to play W when D plays either W or S. All proofs of theorems are provided in [10]. In practice, both macroplayers wait until the last stage where they rely on their respective probabilities p_D and $p_A = 1 - p_D$ to win; both macroplayers actually play S in the last stage.

[3]Although more stages can be included in the model, we consider only 3 stages to keep the analysis tractable. We leave the extension to a general number of stages n to future work.

4.2.2 Incentives

The previous result for $\mathbf{G_{AD}}$ is not desirable because the information verifier can decide on the information only at the deadline. In addition, the defender can win only probabilistically. Hence, it is beneficial to design a version of the game where macroplayers send their attributes earlier (i.e., play S from the beginning). One way to achieve this is to give both macroplayers incentives to play earlier. In this section, we analyze the game with incentives $\mathbf{G^I_{AD}}$. Figure 3 illustrates this game. The only difference with respect to $\mathbf{G_{AD}}$ is that if a macroplayer plays S before the last stage, it receives a reward r (this can be a *bonus* trust level) from the information verifier regardless of whether it wins or loses the game.[4] The resulting equilibrium is not constrained to waiting as the theorem below shows.

THEOREM 4.2. *The PBE of* $\mathbf{G^I_{AD}}$ *is achieved by the following strategies:*

$$
\begin{array}{ll}
(W,W) & \textit{if} \quad r \leq \min\{p_D c, p_A c\} \\
(S,S) & \textit{if} \quad r > \max\{p_D(c+\delta), p_A c + p_D \delta\} \\
(W,S) & \textit{if} \quad (p_D c < r \leq \min\{p_D(c+\delta), p_A c - p_D\delta\}) \\
 & \quad \vee (p_D(c+\delta) < r \leq p_A c + p_D \delta) \\
(S,W) & \textit{otherwise}
\end{array}
$$

To enforce the strategy (S,S), we need $r > \max\{p_D(c+\delta), p_A c + p_D\delta\} \quad \forall p_D \leq 1$. This implies $r > c + \delta$. If $r = c + \delta$ and $p_D = 1$, the best-response strategies are (S,W), but as there is only player D (because $p_A = 0$), (S,W) is equivalent to (S,S) in this case. This justifies not requiring the strict inequality $r > c + \delta$ and leads to the following corollary:

COROLLARY 4.1. *The strategy* (S,S) *can be enforced by choosing* $r \geq c + \delta$.

As both the defender and the attacker can receive the reward r, the amount of the reward should be minimal and still satisfy the condition for enforcing (S,S).

The definition of the last stage in the attacker-defender games merits some clarifications. One of the main questions is "When does the last stage start?" As the probability of successfully sending evidence is 1 until the last stage, we assume that this stage begins when the above probability becomes lower than 1. Determining this exact moment is admittedly difficult, hence there is a possibility that, after one macroplayer plays, the other macroplayer could succeed in transmitting more evidence and surpass the first macroplayer. Although in this case the model of $\mathbf{G_{AD}}$ does not apply anymore, that of $\mathbf{G^I_{AD}}$ does because macroplayers actually send evidence before the last stage. Thus, $\mathbf{G^I_{AD}}$ implicitly models the case when macroplayers incorrectly estimate the beginning of the last stage.

4.3 Trust Contribution Game

The trust contribution game $\mathbf{G_{TC}}$ captures how individual benign rational entities contribute to the defender trust level in $\mathbf{G_{AD}}$. Let $t_k \leq 1$ be the entity-centric trust levels contributed by $K \geq 2$ entities. Each entity has to set the

[4]Further details about the reward mechanism are in [10].

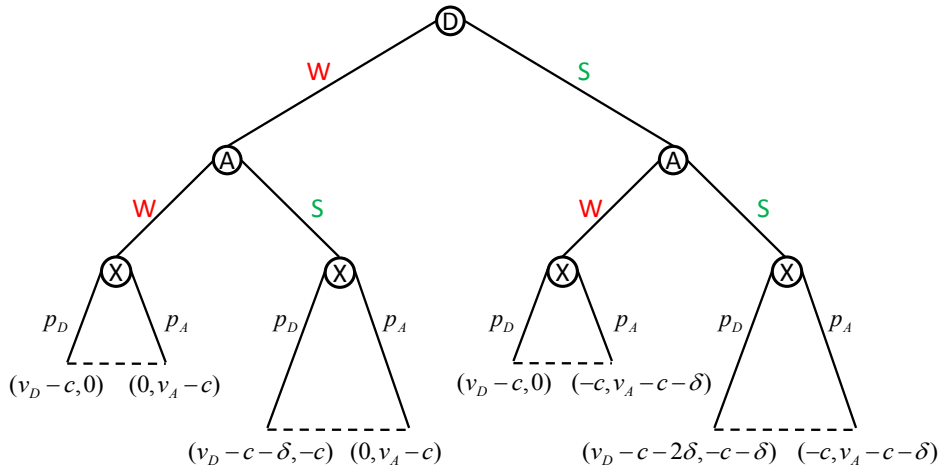

Figure 2: The Attacker-Defender Game $\mathbf{G_{AD}}$. The X in the last node indicates that both macroplayers play in the last stage. The tuples at the leaves of the tree represent the payoffs of the macroplayers; the negative values are the costs (invested privacy) and the positive values are the gains when winning the game. The probabilities of winning are such that $p_D + p_A = 1$. For example, the rightmost leaf of the tree represents the case where both macroplayers play S and A wins. A realizes a gain of v_A at the cost of surpassing D's previous action (D revealed the minimum amount of privacy c) by the increment δ.

value of t_k by providing some private information. Before going into the details of the analysis, we need to define exactly how private information (i.e., attributes) is converted into trust. Let ϕ_k be the *trust-privacy conversion factor*: 1 unit of private information = ϕ_k units of trust. Assuming identical entities, $\phi_k = \phi = 1$. Based on this, the threshold trust and privacy levels are linked as follows: $\theta = \phi c = c$. We assume that entities play sequentially, i.e., they observe the trust levels contributed by previous microplayers. We also assume that entities know the target collective trust level based on the analysis of $\mathbf{G_{AD}}$ above.

4.3.1 Equilibrium

In $\mathbf{G_{TC}}$, the payoff of an entity, in private information units, is:

$$\forall k \in \{1,\dots,K\}, \quad \pi_k(t_1,\dots,t_K) = \frac{v_D}{K} - \frac{t_k}{\phi} \qquad (1)$$

This means that winning $\mathbf{G_{AD}}$ benefits all contributing entities equally (e.g., by avoiding the cost induced by a false information attack), but each one contributes a different level of privacy. To solve $\mathbf{G_{TC}}$, we compute its *Subgame-Perfect Equilibrium* (SPE).[5] The resulting equilibrium is, unsurprisingly:

THEOREM 4.3. *The SPE of $\mathbf{G_{TC}}$ is defined by:*

$$t_k^* = 0$$

In practice, this result means that no entity will contribute in $\mathbf{G_{TC}}$, thus making it impossible to collect the required trust levels in $\mathbf{G_{AD}}$. We solve this problem in the next section.

[5]The SPE is stronger than the typical Nash equilibrium because there is only one SPE equilibrium in a game, whereas there can be several Nash equilibria.

4.3.2 Incentives

Adding incentives to $\mathbf{G_{AD}}$ results in macroplayers sending their attributes in earlier stages of the game (Section 4.2.2). In this section, we investigate the effect of incentives on $\mathbf{G_{TC}}$. Let $\mathbf{G^I_{TC}}$ be the version of $\mathbf{G_{TC}}$ with incentives; $\mathbf{G^I_{TC}}$ corresponds to $\mathbf{G^I_{AD}}$. The payoff of an entity, in private information units, is:

$$\forall k \in \{1,\dots,K\}, \quad \pi_k(t_1,\dots,t_K) = \frac{v_D}{K} + r\frac{t_k}{\sum_{i=1}^{K} t_i} - \frac{t_k}{\phi} \qquad (2)$$

This payoff function takes into account the reward r attributed to the early movers in $\mathbf{G^I_{AD}}$ (i.e., the attacker or the defender). Among the rewarded entities of one group (e.g., the entities constituting the defender), the reward should be distributed proportionally to the individual contributions of these entities to encourage high contributions. The resulting equilibrium solves the problem in Theorem 4.3.

THEOREM 4.4. *The SPE of $\mathbf{G^I_{TC}}$ is defined by:*

$$\forall k \in \{1,\dots,K\}, \quad t_k^* = \frac{\phi r(K-1)}{K^2}$$

We still need to compute r while considering Corollary 4.1. Back to $\mathbf{G^I_{AD}}$, if macroplayer D (the defender) wants to win the game, it should contribute at least $c + 2\delta$ of private information. This results in the following values for r and t_k^*:

$$\sum_{k=1}^{K} t_k^* \geq \phi(c+2\delta) \qquad (3)$$

Substituting t_k^* from Theorem 4.4 and taking into account the requirement that r should be minimal to prevent gener-

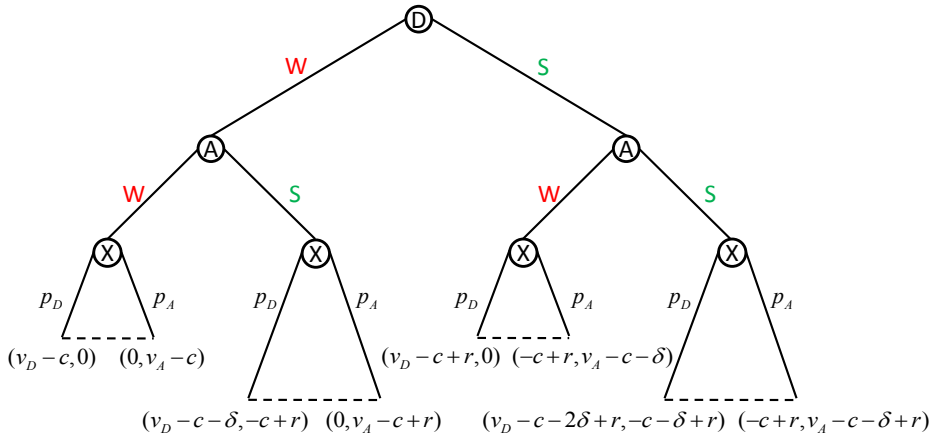

Figure 3: The Attacker-Defender Game with Incentives G^{I}_{AD}. Macroplayers that play S before the last stage of the game receive a reward r.

ously rewarding the adversary, we obtain:

$$r = \frac{(c+2\delta)K}{K-1} \tag{4}$$

$$t_k^* = \frac{\phi(c+2\delta)}{K} \tag{5}$$

Equation (4) satisfies the lower bound condition on r. The upper bound on δ can be computed, based on (5), as follows:

$$t_k^* \leq 1 \Rightarrow \delta \leq \frac{K-\phi c}{2\phi} \tag{6}$$

5. CONCLUSION

In this paper, we optimize the trust-privacy tradeoff under the assumption of privacy-preserving entities that rationally minimize their privacy loss. Using game-theoretic models, we show that individual players do not contribute to trust establishment, unless they receive appropriate incentives. For example, in a network of privacy-preserving nodes, no misbehaving nodes will be revoked by a voting mechanism unless there are incentives for revocation. We believe that explicitly modeling the notion of privacy-oriented rationality will shed additional light on the appropriate mechanisms, such as incentives, for building privacy-preserving systems. We also hope that this work is only the beginning of an effort to bridge privacy and game theory, two fields that share their main focus: realizing the preferences of the human in the loop.

6. REFERENCES

[1] `http://www.w3.org/P3P/`.

[2] A. Acquisti, R. Dingledine, and P. Syverson. On the economics of anonymity. In *Proceedings of FC'03*, volume 2742 of *LNCS*, pages 439–443.

[3] P. Cashmore. Next year's Twitter? it's Foursquare, 2009. `http://edition.cnn.com/2009/TECH/11/19/cashmore.foursquare/index.html`.

[4] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 1991.

[5] J. Halpern and V. Teague. Rational secret sharing and multiparty computation (extended abstract). In *Proceedings of STOC'04*.

[6] R. Jurca and B. Faltings. Collusion-resistant, incentive-compatible feedback payments. In *Proceedings of EC'07*.

[7] J. Katz. Bridging game theory and cryptography: Recent results and future directions. In *Proceedings of TCC'08*, volume 4948 of *LNCS*, pages 251–272.

[8] L. Lilien and B. Bhargava. *Trading Privacy for Trust in Online Interactions*. Idea Group, 2008.

[9] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang. URSA: ubiquitous and robust access control for mobile ad hoc networks. *IEEE/ACM Transactions on Networking*, 12(6):1049–1063, December 2004.

[10] M. Raya. *Data-Centric Trust in Ephemeral Networks*. PhD thesis, EPFL, 2009.

[11] M. Raya, P. Papadimitratos, V. Gligor, and J.-P. Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *Proceedings of INFOCOM'08*.

[12] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of WiSe'03*.

[13] K. E. Seamons, M. Winslett, T. Yu, L. Yu, and R. Jarvis. Protecting privacy during on-line trust negotiation. In *Proceedings of PET'02*, volume 2482 of *LNCS*, pages 249–253.

[14] J.-M. Seigneur and C. Jensen. Trading privacy for trust. In *Proceedings of iTrust'04*, volume 2995 of *LNCS*, pages 93–107.

[15] D. Yao, K. B. Frikken, M. J. Atallah, and R. Tamassia. Private information: To reveal or not to reveal. *ACM Transactions on Information and System Security*, 12(1):1–27, 2008.

[16] S. Yi and R. Kravets. MOCA: Mobile certificate authority for wireless ad hoc networks. In *Proceedings of PKI'03*.