TrustRings in mobile wireless network settings

Dagmara Spiewak, Volker Fusenig and Thomas Engel
University of Luxembourg
Faculty of Sciences, Technology, and Communication
6, r. Richard Coudenhove-Kalergi
L-1359 Luxembourg

Abstract: Trust in mobile wireless networks introduces new challenges in addition to the traditional notions of *Trust* for infrastructure networks. Mobile, wireless and dynamic network settings diversify *Trust* research in multiple ways. Unfortunately, traditional security concepts, such as Public Key Infrastructures, are not accurate to protect sensitive communication in these special network environments. In this work, we focus on *Trust* establishment and calculation in mobile wireless networks, which includes Mobile Ad-Hoc Networks known as MANETs. We present our idea of *TrustRings* which is used to calculate *Trust-Values* for entities in mobile wireless networks. Our model is based on an egocentric network view which is combined with the location and the distance between communicating devices.

Key–Words: Trust, Security, Mobility, MANETs, Network Model

1 Introduction

Mobile wireless ad-hoc networks, including mobile ad-hoc networks (MANETs) and Mesh-Networks, are systems of nodes that interconnect in a dynamically and self-organized way allowing the extension of common Wireless LAN technologies over wide areas with less or even no previously available network infrastructure. However, the nature of mobile wireless networks with its resource-constrained devices makes them very vulnerable to malicious attacks and selfish actions. Particularly due to the absence of preestablished communication infrastructure and the absence of continuously accessible central entities, security in mobile ad-hoc wireless networks is very difficult to reach and to maintain. Nevertheless, confidential data and sensitive applications transmitted within mobile wireless networks require a high degree of security. Therefore, more and more research topics are focusing on the establishment of *Trust-Metrics* in order to overcome this weakness and to ensure secured and reliable communications in these almost autonomous network scenarios of mobile wireless adhoc networks and Mesh-Networks.

The crucial point is, that *Trust* in the field of network security is not clearly defined. The word *Trust* is mostly used intuitively, serving as foundation for follow-on security concepts, such as a basis for public-key management infrastructures. So far, subjective interpretations about the meaning of the word *Trust* lead to big ambiguousness. Pradip Lamsal in [13] and Audun Josang in [11] present a wide expertise on the description of *Trust* as well as its relationship towards *Security*. Beyond, Pirzada and McDonald emphasize in [14] the interdependency of *Trust* and *Security*, while *Security* is highly dependent on trusted key exchange and trusted key exchange on the other side can only proceed with the required security services. Furthermore, the notion of *Trust* in mobility settings is compared to *Trust* applied to the Internet in [4] highlighting the independence of previously build *Trust* infrastructures.

In the following course of the paper, Section 2 presents relevant related work on the establishment and distribution of *Trust-Values* within mobile network settings. Consequently, Section 3 introduces our concept of *TrustRings* to obtain and calculate the *Trust-Value*. Finally, Section 4 concludes the paper.

2 Background and Related Work

Trust in fixed networks One of the most important milestones in the history of cryptography was the concept of *Pretty Good Privacy* or *PGP* [18] making cryptography available to a wide community. Principally created for email-encryption and -signing, *PGP*

functioned as a hybrid cryptosystem based on the concept of *Web of Trust*. Basically, the idea is to allow each user to operate as an autonomous certification authority, enabling them to sign and verify keys of other entities even without a central certification authority. This results in the establishment of various virtual interconnections of *Trust*. However, even though no central authority is needed to sign the keys, the distribution of keys is handled by a continuously accessible directory making *PGP* inadequate in mobile network settings. The core of the famous *Distributed Trust Model* [1] is the *recommendation protocol* which is always launched if the *Trust Value* of a certain network entity is required. Depending on the output of this protocol *Trust* is measured and assigned into categories ranging from -1 (complete distrust) to 4 (complete trust). Distributing recommendations about entities has to be secured from unauthorized modifications and fake recommendation spreading. Unfortunately centralized maintenance and distribution of recommendations is not feasible in mobile network settings. Furthermore recommendation based protocols are very vulnerable to *Sybil-attacks*, which is elaborated in [15]. Therefore, the new *TrustRing* idea, presented in this paper, will not involve or even consider recommended or third-party information to calculate the *Trust-Value* of communication entities.

Audun Jøsang expresses *Trust* as *Beliefs* and uses the method of *Subjective Logic*, introduced in [9], to calculate the *Trust-Value* among arbitrary network entities [10]. Generally, *Belief theory* facilitates the approximate reasoning on trueness of data in situations of incomplete knowledge. However, if we exemplarily consider the scenario of authenticating a network entity B within a mobile wireless network scenario in multi-hop transmission range by another network entity A, we notice that an unbroken chain of *trusted* entities is very essential, to reason about the real identity of B. The assumption of an unbroken chain within wireless and mobile network settings is a critical condition, taking the high vulnerability to wireless link breaks of mobile networks into account [16].

Trust in mobile networks *Trust management* in mobile ad-hoc networks poses several challenges compared to *Trust* in traditional networks like the Internet or common WLAN architectures. Typically, sources of *Trust*, like *Trusted Third Parties* (*TTP*) reside on centralized servers and operate as fully-trusted and continuously accessible *Trust* evidence distribution network entities. Obviously, these centrally managed *Trusted Third Parties* are entirely important for the overall security of the network. Unfortunately these entities produce a single point of failure within the network, which means, that by compromising them, the security of the whole system is broken. Due to the fact that entities of dynamic and mobile wireless networks can be compromised much easier, centrally managed *Trusted Third Parties* are not adequate to function as sources of *Trust* within mobility settings.

Unfortunately, the attractiveness of mobile wireless networks of *anytime* and *anywhere* communication, is always accompanied with weaknesses, such as the breakage of wireless links or the unavailability of services, making centralized management systems inadequate. As a consequence, *Trust* management has to be organized in a distributed way and handled by the network entities themselves. Accordingly, each network entity needs to individually evaluate the *Trust-Value* of another entity without referring to a global *Trust-Value* assignment system.

One recent work on *Trust* computation and distribution in mobile and dynamic networks was introduced by Tao Jiang and John S. Baras [7]. It presents a methodology for distributing *Trust-Certificates* called *ABED (Ant-Based Evidence Distribution Algorithm)* by utilizing the idea of Swarm Intelligence Paradigm [3]. The proposed algorithm generates ants every time a certain certificate, which serves as a *Trust* evidence, is required. The main weakness of the ABED approach is its high vulnerability to Denial-of-Service attacks [15]. After a detailed analysis of the model it is noticeable, that a malicious network entity has the capacity to send a huge amount of certificate requests for non-existing certificates simultaneously by spreading ants into the network.

One very famous *Trust* model is the *EigenTrust* algorithm described in [12]. It proposes the establishment of *Trust* within Peer-to-Peer networks. Like in dynamic mobile networks, a centralized *Trust* management in Peer-to-Peer is not possible as well. The *EigenTrust* algorithm helps to reduce the amount of not authentic files within the system even in the presence of collaborating adversarial network entities. In order to reach their aim, the authors assume several peers as *pre-trusted* from the outset. These *pre-trusted* entities might be the initiators of the network. One interesting aspect of this approach is the generation of a global *Trust-Value*. This value represents how much all network entities trust one specific network node. This global *Trust-Value* is based on local *Trust-Values*,

collected from either positive or negative transactions. The main weakness of the *EigenTrust* model is the precondition of *pre-trusted* network entities. Nevertheless, the overall idea of the *EigenTrust* algorithm might be enhanced and tailored to the dynamic nature of mobile wireless networks, by introduction of a random as selection of the *pre-trusted* entities. The more serious problem of the algorithm represents the calculation of the global *Trust-Value*. The collection of information, or here the collection of local *Trust-Values*, implicates multiple vulnerabilities to security problems in mobile network settings. One of them is known as the *Sybil-attacks*. In order to avoid these attacks each of the local *Trust-Values* hat to be communicated over authenticated channels. This is a critical condition, taking the high vulnerability to wireless links breaks in mobile network settings into account. For that reason, the newly elaborated concept of *TrustRings*, which is going to be presented in the following section of this paper, is completely independent of globally calculated *Trust-Values*.

In contrast to the *EigenTrust* algorithm the authors in [8] assume that *Trust* is handled completely distributed and that *Trust* is only restricted to local interactions. Keeping this idea in mind, they model the mobile network as an undirected graph (V,E). The edges represent connections to exchange trust information. This means that two end-nodes of an edge might not be physical neighbors in geometrical distance although they have a trust relationship in the graph. The distributed trust computation model is based on elementary voting methods, so that only entities in the neighborhood have the right to vote about the trustworthiness of a network entity. An entity tries to find the most trusted nodes in order to generate a secure path for communicating to another entity. Unfortunately, this *Trust* model is very vulnerable to *Sybil-attacks* as well. The attacker may fake opinions about the trustworthiness of a certain node in order to attract more traffic to it and compromise the node.

In the following section we will model the network and present the idea of *TrustRings*. We use the model to calculate *Trust-Values* in mobile and dynamic wireless network settings.

3 TrustRings Network Model

Basically, the *TrustRings* network model can be represented as an egocentric network model, like demonstrated in Figure 1.

The TrustRing Network Model procedure is performed by each node in the network autonomously in the following way: Placing itself as the centric node in the middle of the network, first of all each node starts to build 3-dimensional spheres around itself using the multiple its own transmission range as the radius of the sphere. According to this, the first sphere of a node is created by using exactly the transmission range (maximum 1-Hop distance) of the node. The model assumes that all nodes have the same transmission range, so that the nodes' spheres at the same Hop-distance have equal dimension.

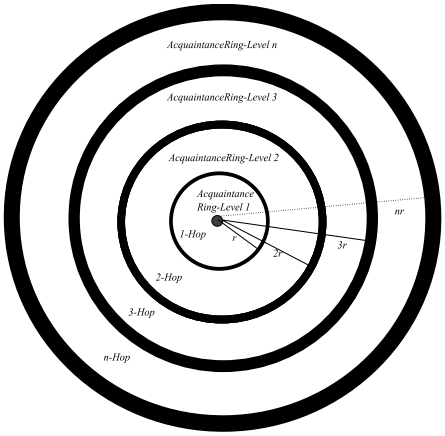

Figure 1: TrustRings network model

Continuing this process, the next sphere of each node is created by using the doubled transmission range (maximum 2-Hop distance), the third sphere is generated applying the triple transmission range (maximum 3-Hop distance) and so on. Figure 1 visualizes a reduced 2-dimensional view of the *TrustRing* Network Model, where spheres are represented simply as rings leading to the name of the model.

All entities within the direct (1-Hop) range from the centric node are located within the innermost sphere, named *AcquaintanceRing-Level 1*. The subsequent sphere, which is generated by the centric node, is called *AcquaintanceRing-Level 2*. By further iterating this process, *AcquaintanceRings* of different levels are generated, such as in *n-Hop* distance from the centric node the *AcquaintanceRing-Level n* sphere is located. However, the assumption that a centric node *i* can communicate with node *j*, which is located within *i*'s *AcquaintanceRing-Level 2*, by investigating 2 Hops to bridge the distance by the help of an intermediate node *k*, where node *k* forwards the packet to the required destination node *j*, is generally **wrong**.

Although, node *j* is located within *i*'s *AcquaintanceRing-Level 2*, it is still not guar-

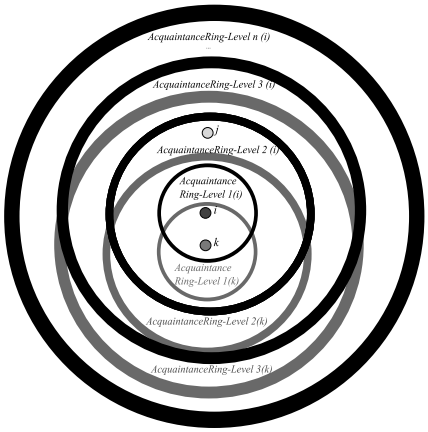

Figure 2: Multi-Hop communication

anteed that a 2-Hop route is available towards node *j* even though node *k* resides within the *i*'s *AcquaintanceRing-Level 1*. Figure 2 presents an accurate example for this phenomenon. For this reason, only nodes within node *i*'s *AcquaintanceRing-Level 1* can be reached with 1-Hop communication.

3.1 Trust calculation

In addition to the egocentric view of the network, each network node *i* maintains a *Trust-Value-Database* to store the *Initial-Trust-Value* $\eta_{(i,j)}$ from known network entities that are labeled by an unique natural number j. As the name indicates, the *Initial-Trust-Value* $\eta_{(i,j)}$ is not the only *Trust-Value* a node *i* can have of a network entity *j*. This *Initial-Trust-Value* $\eta_{(i,j)}$ is calculated by node *i* only from **direct** and local interactions with the entity j within node *i*'s *1-Hop* communication range (or in other words within node *i*'s *AcquaintanceRing-Level 1*). Obviously, positive experiences with node *j* raise the *Initial-Trust-Value* $\eta_{(i,j)}$ whereas negative experiences with node *j* lead to a smaller *Initial-Trust-Value* $\eta_{(i,j)}$. Nodes have the ability to decide by themselves how they evaluate positive and negative experiences. Each node may use its own metric to calculate the *Initial-Trust-Value* $\eta_{(i,j)}$.

In any case, the *Initial-Trust-Value* is very essential and builds the foundation for all succeedingly calculated *Trust-Values* of the specific node to which the *Initial-Trust-Value* belongs to.

Depending on the distance of the *TrustRing* a network entity *j* is located from the centric node *i*, the *Trust-Value* $\eta^{(l)}_{(i,j)}$ (where l is the level-number of node *j*'s *AcquaintanceRing*) decreases exponentially starting from the *Initial-Trust-Value* $\eta_{(i,j)}$. Hence, the farther the location of node *j* the smaller its *Trust-Value* and the uncertain the reliable communication between *i* and *j*. Principally, the shrinking control over the communication together with high vulnerability to wireless link breakages, makes communications towards nodes located within *AcquaintanceRing* of higher levels *l* more susceptible to breakdowns and malicious attacks. As a result, it is very important for the centric node *i* to adjust the *Initial-Trust-Value* $\eta_{(i,j)}$ of node *j* according to the geographical location represented as *AcquaintanceRing* of a certain level. Furthermore, the decreasing control during communications between the centric node *i* and a node *j* leads to an increasing dependence on services of intermediate-nodes *k*. These services might include, for example forwarding of packages or participating in the resolution of route-requests. The following function in Definition 1 can be used to calculate the node *j*'s *Trust-Value* in different levels of *AcquaintanceRings*, if and only if the *Initial-Trust-Value* is already known from direct and local interactions between node *i* and *j*.

Definition 1 *For a centric node i in a mobile wireless network, let* $\eta_{(i,j)}$ *be the Initial-Trust-Value of network entity j within the AcquaintanceRing-Level 1 (j is located in 1-Hop distance from i). Then the Trust-Value for j, if j is located within i's AcquaintanceRing-Level n, in minimum (n-1)-Hop distance and maximum n-Hop distance from i, is calculated by i with the following function:*

$$\eta^{(n)}_{(i,j)} = \eta_{(i,j)} * e^{(-0.5(n-1))}, \textit{ where } n \in 1, 2, 3, ...$$

Figure 3 highlights the influence of the *Initial-Trust-Value* $\eta_{(i,j)}$ of a certain node *j* calculated by the centric node *i* for the subsequent calculation of the *Trust-Values*.

It is noticeable that the *Trust-Values* of the functions with the *Initial-Trust-Value* $\eta_{(i,j)}$ ranging from 1 to 5 fall below 1 already after the 4^{th} Hop. By doubling the *Initial-Trust-Value* $\eta_{(i,j)}$ up to 10 the curve will fall below 1 after the 5^{th} Hop. By reapplying this process to the *Initial-Trust-Value* of 20, 6 Hops are sufficient to compute a *Trust-Values* below 1. By further increasing the *Initial-Trust-Value* up to 100 the curve will fall below 1 after the 10^{th} Hop, illustrated in the table below.

Deciding to select 20 for the maximum *Initial-Trust-Value* $\eta_{(i,j)}$ will allow up to 6 Hops until the

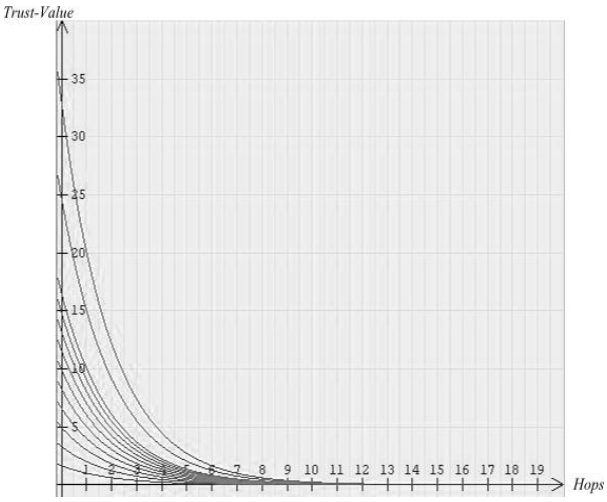

Figure 3: Trust-Value: family of functions

Trust-Value will fall below 1. This aligns with practical results from simulation of, for example the topology-based routing protocols for mobile ad-hoc networks, like the *Virtual Topology Based Routing Protocol* [2], that operates up to an average Hop-bound of 4. Choosing too high values for $\eta_{(i,j)}$ results in unrealistic maximal Hop-bounds and simultaneous implications of unreliable communication due to the dramatically decrease of bandwidth within the mobile ad-hoc network [5]. This leads to the conclusion that the *Trust-Values* can range from 0 to 20 basing on previous interactions and experiences.

3.2 TrustRing discovery

In the event, node *i* needs to calculate or lookup the accurate *Trust-Value* $\eta^{(n)}_{(i,j)}$ of node *j* in order to communicate within the mobile wireless network, *i* needs to determine the level of the *AcquaintanceRing* node *j* is located. This process has to be performed very carefully, because the *Trust-Value* of *j* decreases with increased level of the *AcquaintanceRing* exponentially. We assume that each network entity has an unique IP address assigned, by the use of the *Distributed Protocol for Dynamic Address Assignment* [17]. Furthermore, it is obvious that in the event an entity *i* wishes to communicate with network entity *j*, *i* knows the IP address and the *Initial-Trust-Value* $\eta_{(i,j)}$ of *j*. In order to calculate *j*'s *Trust-Value* it is sufficient for entity *i* to discover the level of the *AcquaintanceRing*, in which *j* is located. It is not necessary to determine concrete coordinates of entity

Table 1: Trust-Values depending on the number of hops from center-node i and on the Initial-Trust-Value $\eta_{(i,j)}$

# Hop	$\eta_{(i,j)}$ 1	2	3	5	10	20	100
1	1	2	3	5	10	20	100
2	0.6065	1.2131	1.8196	3.0327	6.0653	12.120	60,653
3	0.3688	0.7358	1.1036	1.8394	3.6788	7.3576	36,788
4	0.2231	0.4463	0.6694	1.1157	2.2313	4.4626	22,313
5	0.1353	0.2707	0.4060	0.6767	1.3533	2.7067	13,533
6	0.0820	0.1642	0.2463	0.4104	0.8209	1.6417	8,209
7	0.0498	0.0996	0.1494	0.2489	0.4979	0.9957	4,979
8	0.0302	0.0604	0.0906	0.1510	0.3020	0.6040	3,020
9	0.0183	0.0366	0.0550	0.0916	0.1832	0.3663	1,832
10	0.0111	0.0222	0.0333	0.0555	0.1110	0.2222	1,111
11	-	-	-	-	-	-	0,674

j, because the *Trust-Value* remains equal within the whole *AcquaintanceRingArea* at the same level. One efficient mechanism was invented by Stephen Mark Huffman and Michael Henry Reifer and patented by the *United States Patent*, which allows to geolocate logical network addresses [6]. This technology requires stationary network entities in order to be able to create the so-called *Network Topology Map*. Unfortunately, mobile ad-hoc networks are established on-the-fly without a pre-existing network infrastructure but with permanently changing and dynamic topology. Therefore, a mobile wireless network is highly dependent on cooperative behavior from network entities within their most trusted area, which is the *AcquaintanceRing-Level 1*. Consequently, in order to locate the level of the *AcquaintanceRing* of entity *j*, the network centric node *i* interviews the nodes within its *AcquaintanceRing-Level 1*, if they have any information about the location of *j*, or *i* requests them to forward the location-request message *LocReq* to their most trusted nodes within their *AcquaintanceRing-Level 1*. In return for their service, entity *i* increases the *Initial-Trust-Value* $\eta_{(i,k)}$ of the nodes *k* who participated in the *j*-location request process.

4 Conclusion and Future Work

We have introduced the procedure of *TrustRings* which facilitates the calculation of *Trust-Value* for entities in mobile wireless networks. The core of the presented methodology represents an egocentric view of the network. According to this concept each node generates 3-dimensional spheres around itself, using the multiple of its maximum *1-Hop* transmission range as radius. Hence, the *TrustRings* idea allows network entities to compute the *TrustValues* towards other network participants dynamically. Based on a previously created *Initial-Trust-Value*, which is obtained by observing and measuring the *good* and *bad* experiences with the other network entity, the actual *TrustValue* is calculated in relation to the location and distance of nodes by using the idea of *TrustRings*. Primarily, the advantage of the *TrustRings* Network Model compared to other solutions, analyzed in section 2 of this paper, is primarily its complete independence of for example recommended third-party *Trust-Values*. As a result, the *TrustRings* Network Model is resistant to *Sybil-attacks*. In our future work, we are going to implement and complete the *TrustRings* Network Model. Furthermore we will investigate on the exact computation of the *Initial-Trust-Value* where we will take third-party *Trust-Values* from *Trust-Databases* into account.

References:

[1] A. Abdul-Rahman and S. Hailes. A distributed trust model. *Proceedings of the 1997 workshop on New security paradigms*, 1997.

[2] I. F. Akyildiz, J. I. Pelech, and B. Yener. Virtual topology based routing protocol for multihop dynamic wireless networks. *Wireless Networks, Volume 7 , Issue 4 (August 2001)*, pages 413 – 424, 2001.

[3] B. Awerbuch, D. Holmer, and H. Rubens. Swarm intelligence routing resilient to byzantine adversaries. 2004.

[4] L. Eschenauer, V. D. Gligor, and J. S. Baras. On trust establishment in mobile ad-hoc networks. *ACM Conference on Computer and Communications Security*, pages 41–47, 2002.

[5] L. Georgiadis, P. Jacquet, and B. Mans. Bandwidth reservation in multihop wireless networks: Complexity and mechanisms. *24th International Conference on Distributed Computing Systems Workshops - W6: WWAN (ICDCSW'04)*, pages 762 – 767, 2004.

[6] S. M. Huffman and M. H. Reifer. United states patent: Method for geolocating logical network addresses (6,947,978). 2005.

[7] T. Jiang and J. S. Baras. Ant-based adaptive trust evidence distribution in manet. *Proceedings of MDC*, 2004.

[8] T. Jiang and J. S. Baras. Cooperative games, phase transition on graphs and distributed trust in manet. *In Proceedings of 43rd IEEE Conference on Decision and Control*, 2004.

[9] A. Josang. An algebra for assessing trust in certification chains. *Proceedings of the Network and Distributed Systems Security*, 1999.

[10] A. Josang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. *Proceedings of Australasian Computer Science Conference*, 2006.

[11] A. Josang, C. Keser, and T. Dimitrakos. Can we manage trust? *Proceedings of iTrust*, 2005.

[12] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. *In Proceedings of the Twelfth International World Wide Web Conference*, 2003.

[13] P. Lamsal. Understanding trust and security. *Department of Computer Science, University of Helsinki, Finland*, 2001.

[14] A. A. Pirzada and C. McDonald. Establishing trust in pure ad-hoc networks. *ACM International Conference Proceeding Series; Vol. 56*, pages 47 – 54, 2004.

[15] D. Spiewak and T. Engel. Trust as foundation for follow-on security mechanisms in manets. *WSEAS Transactions on Communications, Issue 1, Volume 6*, pages 125–131, 2007.

[16] D. Spiewak, T. Engel, and V. Fusenig. Unmasking threats in mobile wireless ad-hoc networks settings. *WSEAS Transactions on Communications, Issue 1, Volume 6*, pages 104–110, 2007.

[17] M. R. Thoppian and R. Prakash. A distributed protocol for dynamic address assignment in mobile ad hoc networks. *IEEE Transactions on Mobile Computing Vol. 5, No. 1*, pages 4 – 19, 2006.

[18] P. R. Zimmermann. The official pgp user's guide. *Department of Computer Science, University of Helsinki, Finland, MIT Press*.