Review and Reputation based Trust Score Calculation for WLAN (RRTSC)

Amruta B. Pandule, Poonam N. Railkar, Parikshit N. Mahalle
Department of Computer Engineering
STES's Smt. Kashibai Navale College of Engineering
Pune - 411 041 India.

ABSTRACT
Wireless networks are becoming more and more popular nowadays. These are widely used because they are easy to deploy. As these networks are essentially decentralized in nature they enhance the resource sharing and collaboration. The anonymous and open nature of system offers an almost ideal environment for unauthorized access of resources and also prone to different attacks in the network. These systems have to challenge the attacks like man-in-the-middle, replay and Denial of Service (DoS) attacks by anonymous malicious peers. So these systems have to protect themselves from these malicious nodes. For this purpose, before communication happens node must determine whether other nodes are trusted and in turn authorized to access resources or functionalities i.e. nodes must establish the trust before their interactions. Hence there is a need to have an effective Trust Management System which will establish a trust between the nodes in a network will update it periodically. This paper presents novel trust management model for trust score calculations to achieve trusted communication in WLAN network.

This paper proposes a Review and Reputation based Trust Score Calculation (RRTSC) scheme for wireless networks and independent ad-hoc networks. This presents the trust based model for WLAN as an example of scenario of central authority assisted network which compute the trust for a node based in WLAN. In this trust establishment and trust maintenance between the two peers in WLAN is achieved by trusted central authority.

General Terms

Security, Attacks.

Keywords
Trust, Reputation, Trust Management System.

1. INTRODUCTION
P2P networks are very useful in accelerating the communication processes and reducing the collaboration costs but sometimes with untrusted and unreliable nodes in the network. So there is P-trust model which parameter estimation based model [1] for maintaining the trust information of the other nodes in the network.

Wireless LANs organizations don't have to setup of wired LANs, with any kind of physical connection between them. These systems are increasingly accepted by more and more people as they provide such an infrastructure that reduces the setting cost of network. WLAN allows any node to share resources maintaining the anonymity. There is 802.11 standard from IEEEE and this specifies the WLAN in three types.

- ***Infrastructure Mode:*** Each WLAN workstation (WS) communicates to any machine through access point (AP) .It may be in same WLAN or connected to outside world through AP.
- ***Ad Hoc network Mode***: Every node talks to another node directly.
- ***Mixed Network Mode:*** Every node can work in the above two modes simultaneously. This is Extended Basic Service Set.

Contrary 820.11's claims, WLANs have very less security. The open and unrestricted environment of WLAN architecture makes it an ideal environment for unauthorized access to resources and information and also for the attackers to spread malicious content. It has to protect themselves from the attacks by anonymous malicious peers. Node must determine whether other Nodes are authorized to access resources or functionalities. Therefore peers involved must establish trust before transaction happens between them.

So the remedy is,

Don't Trust anybody!!!!!!!!

The trust is defined in various terms in various models [21], [11]. In this we have considered the trust in network as the degree of belief about another node. Here trust is considered as a measurable belief and is relative to some transactions. The trust between nodes is directed for e.g. If node A trusts node B but node B may distrust node A. Trust exists and evolves in time. The facts that node A trusted node B in past does not itself guarantee that A will trust B in future. The performance of B and other relevant information may lead A to re-evaluate her trust in B in future.

This paper presents the Trust Management model for central-authority-assisted WLAN which will collect the review of the node before the node enters the network and will periodically monitor its trust values by colleting periodic review from the access points and also will consider the self review. The actual novelty of the model lies in (a) Review collection, (b) Reputation Calculation, (c) Trust Score Calculation based on review and reputation.

2. MOTIVATION
The current Trust Management Model is a generic Trust Management Model for peer to peer networks and ad-hoc networks [21]. It mainly considers the reputation of the node and the recommendations as well as basic properties of trust like asymmetry, reflexivity, transitivity.

There is trust based identity management for WLAN with 802.11 which will consider the review and reputation based trust calculation for node before joining the subnet but there is no monitoring of workstations after entering the network [2]. Evaluation of trust value and trust level is changeless forever. For example a malicious node may enter the WLAN by pretending very honest and pure operation on any of the other node in the network. But once it gets entry in network it starts misbehaving and shows deviation in its intended behavior. This malicious node once entered in network starts attacks on this WLAN.

It may cause

1. The flooding of the network with traffic chocking the transmission lines and preventing other legitimate user from accessing the services in the network. (Denial-of-Service attacks)
2. The attacker can gather sensitive data from network by introducing rogue access point in the WLAN network coverage area.(Rogue network)
3. This malicious node may act as a 'Man-in-the-middle' between two nodes and can change the content of emails, data transactions and instant messages between two nodes.
4. Also this newly added node may pull the valid traffic from WLAN to the wired network for attacking and then reinserting the traffic into proper network, this will redirect the transactions of the stations (Station redirection).

There are many other attacks too which can affect the network. So the motivation is to build the Trust Management model which will establish the trust before the communication starts and will monitor the behavior of all the nodes to update their trust values and trust levels periodically.

3. RELATED WORK

Lot of work has been done in trust-management area. Several trust-management systems have been proposed in recent years for P2P network. Basically the trust management system is classified into three types as Reputation based Trust systems, Policy based Trust systems and Social network based Trust systems.

The Reputation based Trust systems include systems like XRep [3], DMRep [4], EigenRep [5], P2Prep [6]. These systems mainly involve trust evaluation based on measuring the reputation of the peer. To compute the trust value of the given peer the witnesses who have interacted with the same peer in past share their experience with that peer and help to compute the trust rating of the given peer. While computing the trust values they consider two types of ratings as Transaction-based rating (TR) and User-Based Rating (UR). Transaction-based rating is based on direct interaction with another peer for whom trust value is to be calculated and is generated every time when a transaction happens. A node's User-based rating is the rating given by its witnesses according to the previous experience with the given peer. Thus Reputation-based trust systems evaluate the trust in the peer and the trust in reliability of the reosource. K. Aberer and Z. Despotovic [7] proposed a trust Management System that addressed the problem of data management and semantic level. Google's page rank algorithm can also be considered as a global reputation system.

Social Network based trust systems are based on the social relationship between the peers .The evaluation of the trust is based on the analysis of the social network. It includes the different systems like Marsh [8], NodeRanking [9]. Google's PageRank algorithm [10] can also be considered as a global reputation systems. This algorithm does not require the participation of the users to rank the web pages. Basically, the web page with more back links (links that point to it) is considered to be more important (has higher rank) than the one with fewer back links. Page Rank algorithms is also modified and used in social networks for the reputation of the peers. Use of the Bayesian Approach is also proposed in [12], [13]. In these systems, the a posteriori reputation value of a peer is computed combining its a priori reputation values with the new ratings received for the peer. Further, a threshold method is used to determine and update the report reliability of the rater peers. Finally, [14] proposed to use the Cluster Filtering method for reputation systems to distinguish between the reliable and unreliable raters.

The Policy based Trust systems mainly use credentials verification to establish the trust relationship for access control. These systems are based on the notion of delegation, whereby one peer entity gives some of its authority to other peer entity. Some of the policy based trust systems are SPKI [14], KeyNote [15]. Role Based Access Control (RBAC) [16] is also a Policy based Trust system which allows users access to peers based on their responsibilities in the network.

3.1 Evaluation of related work

A lot of work has been done on Trust Management System. With this, the previous work is analyzed and according to our context of research the common parameters have been taken for evaluation of the trust. Table 1 given below shows the evaluation of state of art. For this purpose, this paper considers these parameters in the proposed architecture which have not been considered in the literature.

In this proposed architecture recommendation of the previous node, transaction history of the node which will include how many successful and failure transactions it had , reputation based on the review from all other nodes and finally its own review which is nothing but the reflexivity property of the trust are combined to calculate the trust value for the particular node. The table 1 shows the evaluation of the related work in the form of parameter consideration.

4. PROPOSED SYSTEM

WLAN represents the unique issues based on the fact that the radio signal strengths .As there is no wiring to define membership, this open air nature of WLAN makes it prone to more security threats as discussed above. Therefore it is necessary to secure WLAN through Trust Management which will consider the reputation and it's review from the other node who already had transaction with this node. Thus the Trust Management which will collect the review of the node and compute the reputation based on its transaction history and all other parameters like its self review. And this computed Trust value need to be updated periodically as the node may pretend just to get the entry in the network and then may start misbehaving. So the Trust management model which will establish the trust before communication starts and will monitor the calculated trust periodically need to be developed.

In this section the how review and reputation based trust score is calculated for WLAN is explained briefly. Here assumption is that WLAN model has one central coordinator on

distribution system whose role is to allow or disallow a new wireless node to enter the network. The whole model will work in following three steps

Table 1: Evaluation of related work

Existing model	Identity Authentication	Recommendation	Transaction History	Reputation	Reflexivity (Self Reviews)	Review
[16]	√	ɤ	ɤ	ɤ	√	ɤ
[17]	ɤ	√	ɤ	√	ɤ	ɤ
[18]	ɤ	√	√	ɤ	ɤ	√
[19]	ɤ	ɤ	√	√	ɤ	ɤ
[20]	ɤ	√	√	√	ɤ	ɤ
[21]	√	√	ɤ	√	√	ɤ

√Corresponding parameter is considered in given Trust Management Model

ɤ: Corresponding parameter is not considered in given Trust Management Model

(a) Review collection (b) Reputation Calculation, (c) Trust Score Calculation based on review and reputation. The Admission decision for a new node will be taken by coordinator based on its review received from the nodes which had already transaction with it. Node has to specify what operations want to perform with after joining the network. And after entering the network its trust is monitored periodically so the new node have to prove and maintain its trust level.

Let's consider a WLAN with four different workstations connected to an Access Point (AP) depicted by Fig 1. Each node will be assigned a key pair for encryption and decryption for its, communication with AP. This key pair will be valid for certain time and it has to be renewed. If node has completed the intended task its trust value increases. So based on the trust value duration of the validation of key pair can be made longer. In this model coordinator is chosen among the nodes in the network which will receive the final reputation of the node from the AP. AP have calculated this reputation based on the feedback from all the other nodes. Coordinator will also receive a self review from each node i.e. how much of its intended operations it has completed, what resources it used etc. Coordinator will combine this self review with the reputation send by the AP about particular node in order to calculate the trust score for that particular node. In order to monitor the AP's misbehavior 'reverse monitoring' is done i.e. each wireless node will generate a review report for its AP and will send it to coordinator. This will help to decide trust on AP's review for the nodes. Now the three steps of the architecture come into picture for monitoring of the trust once it has started the transaction in network.

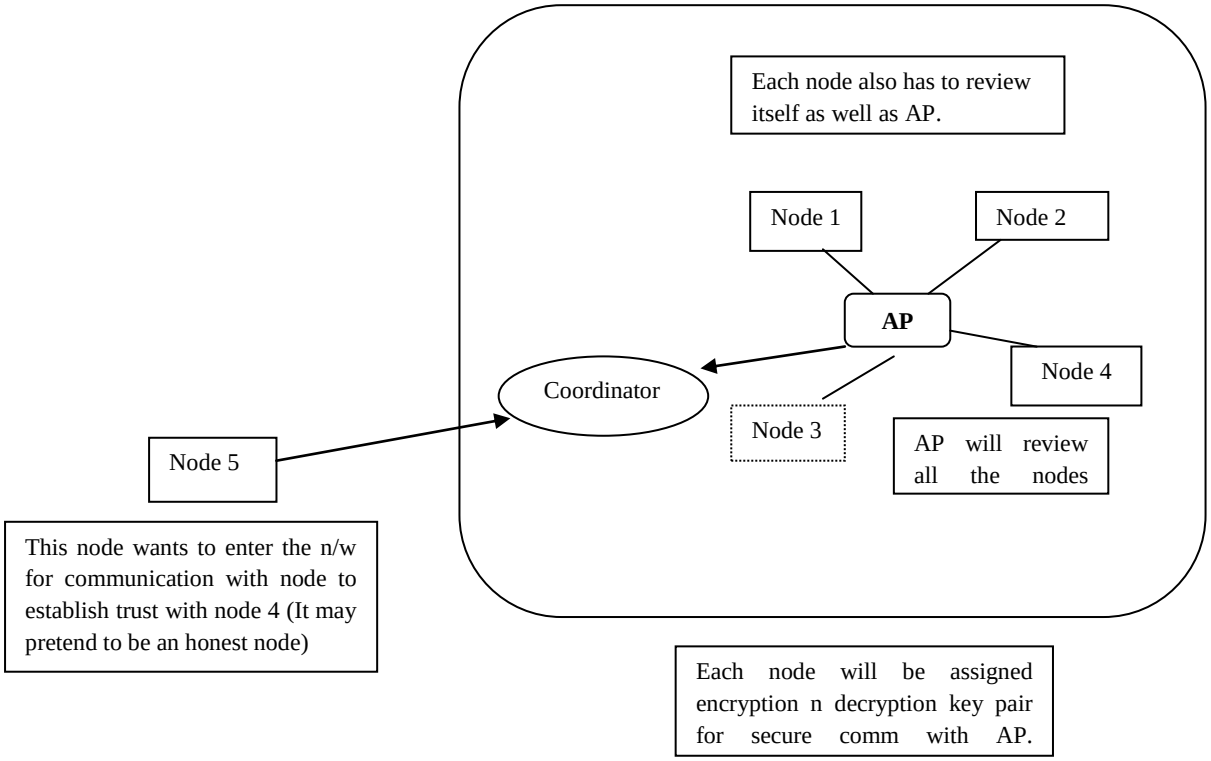

Fig 1. WLAN Networ

1. **Review collection**: For any node Coordinator will consider the self review of the node and review of the node by AP. Now AP will review the node based on the transactions it had in the network. Factors like amount of the data exchanged with AP by node, no of successful transactions of the node, time taken to complete the intended operation .Then AP will send its calculated review to the coordinator node.
2. **Reputation Calculation:** For reputation calculation we will consider the direct trust value of the node and the recommendation trust value. For this two types of rating are considered first transaction-based rating which is based on its direct interaction with another node and is generated every time when a transaction happens. Second user-based rating is the feedback given by the node that already had transaction with particular node based on its performance.
3. **Trust Computation and monitoring:** For the trust computation and monitoring this model will maintain the trust values in the range of (-1, 0, 1) which will represent three trust levels as low, medium and high . Only the nodes with high trust values will be able to perform the operation whose result might have critical impact on the functioning of the network. Once the node goes on completing its intended operations its trust level will be updated.

4.1 Use case Diagrams for the RRTSC

Here in first scenario AP will periodically reviews the performance of the nodes with whom it is connected considering transactions of the node, data exchanged with node and the time taken by the node to complete the intended operations. It will send the review to the coordinator.

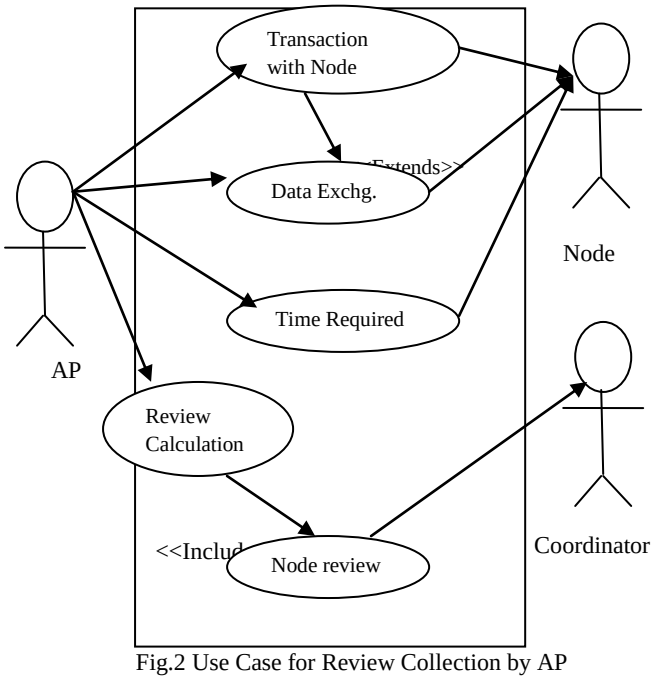

Fig.2 Use Case for Review Collection by AP

In second scenario node will also send its report periodically to the coordinator node i.e. how much of its intended operations it has completed, no of resources it utilized for completion etc. Considering both the reviews coordinator will monitor and update the trust value of particular node periodically.

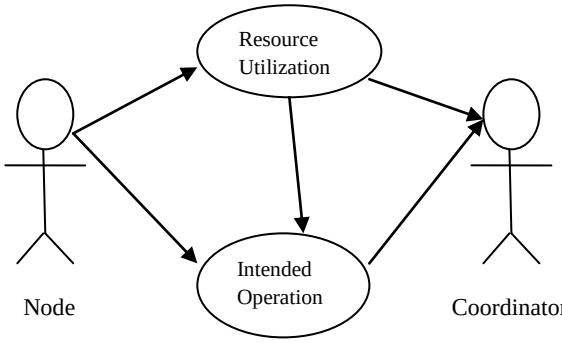

Fig.3 Use Case for self review by Node

Actors:

AP: Access point

Node: One of the nodes in the network

4.2 Proposed RRTSC Algorithm

Let T (i, j) <- Trust value of node i that has for node j. AP will send the review of all the nodes connected with it by combining their feedback from their witnesses. If n will be the no of successful transactions of the node in the network and Tr is the data exchanged between the nodes It can be information downloaded and uploaded between the nodes then for each node following algorithm is followed.

Then there can be two cases while calculating the trust value of the host node.

1. Direct trust of the host node's belief on other node's capability, honesty and reliability based on its own transaction which will depend on the n successful transactions of both nodes.
2. Indirect trust will be trust calculated from the recommendations of the other nodes which had already transactions with host node. This review can be collected from k no of witnesses this number of witnesses can be fixed by the node.

Then the overall trust value of the node can be considered as a trust value of the particular node.

So the direct trust value we are calculating by using Beth et al's formula, which is used to estimate a node's trust in an open network [23].

$$\boldsymbol{T(i,j) = (1-\alpha)\text{^}n} \qquad \textbf{(1)}$$

Where T (i, j) trust value of node i has for node j, α is considered as the transaction rate between the interval (-1 to 1) and n is the no of successful transactions of node i with node j.

For review collection from the different nodes **revCollection** function will calculate the reputation of the given node based on the feedback got from no of witness nodes. It will take the input as no of witness nodes k, n is the no of successful transactions of the witness nodes with the node. Initially the

reputation value will be assumed as zero. For the revCollection for the node it will go to the step 1 with initial rep value as zero.

1] Rep = 0;
A] For (l=0; l< k; l++)
{
A.1] If (n > 0) {

T= (1-α) ^ n
Goto A.2
} else {
T=0 // the trust value of the node is unknown for new node
}

A.2] Rep = Rep + $(T(i,t) * T(t,j))/k$
}
B] Return rep

This **revCollection** function will return the rep which will be then passed as a parameter for trustScoreCalculation function to calculate the trust value for the node which will combine both its direct and indirect reputation to have its final trust value.

This trustValue will not be permanent it may increase or decrease depending on the behavior of the node.

Let's have a set L of trust levels whose elements present the degree of the trust values which can range from -1 to 1. Thus the value between -1 t o 0 shows the distrust i.e. a trust relation can't be established with the node i.e. trustee node has very bad reputation. The value 0 shows that coordinator doesn't have any review for this node i.e. trustee node is completely new for it. The value between 0 to 1 shows that trust relation can be established with the trustee node.

5. CONCLUSIONS AND FUTURE WORK

In this paper, A Review and Reputation based Trust Score Calculation for wireless LAN has been proposed. This architecture is for establishment of the trust for a newly entering node in the WLAN network. In this network the behavior of the node will be monitored periodically and its trust value is also updated .So depending on the behavior of the node in the network trust relation will be established between two nodes.

This paper presents algorithm for RRTSC and also RRTSC scheme is further explained with the help of use case diagram.

Current and future work includes the implementation of the complete system considering all the parameters mentioned in order to have better Trust Management System for WLAN in order to provide the better security.

6. REFERENCES

[1] S. Chen Y. Zhang G. Yang Nanjing University of Posts and Telecommunications, Nanjing, People's Republic of China "Parameter-estimation based trust model for unstructured peer-to-peer networks", The Institution of Engineering and Technology 2011

[2] "Reputation-based Trust Update in Network Environment" Shufen Peng, Jingsha He and Yao Meng , International Symposium on Electronic Commerce and Security, 2008

[3] F.Cornelli, E.Damiani, S.C. Vimercati, S. Paraboschi, and P. Samarati, "Choosing reputable systems in a P2P network". In the proceedings of the eleventh international conference on World Wide Web, Honolulu ,Hawaii ,USA, 2002.

[4] DMRep- K.Aberer, Z. Despotovic, "Managing Trust in peer to peer Information System", In Proc of the IX International Conference on Information and Knowledge Management, Atlanta, Georgia, 2001.

[5] D.kamvar, Mario T. Schlosser, "Eigen Trust Algorithm for Reputation Management in P2P networks", May 2003, ACM 1-58113-680-03/03/0005

[6] F. Cornelli, E.Damiani, S.C. Vimercati, S. Paraboschi, and P. Samarati, "A reputation based approach for choosing reliable resources in Peer to Peer networks", In CCs'02,Washington DC,USA,2002.

[7] K. Aberer and Z.Despotovic ,"Managing Trust in peer-2-peer Information System", Tenth International Conf in Information and Knowledge management 2008

[8] S Marsh "Formalising Trust as a Computational Concept", Ph.D. Thesis University of Stirling.

[9] J. Pujol, R. Sanguesa, "Extracting reputation in multi gent systems by means of social network topology", First International Joint Conference on Autonomous Agents and Multi-Agent Systems, Bologna, Italy.

[10] L. Page, S. Brin, R. Motwani, and T. Winograd, "The Pagerank Citation Ranking: Bringing Order to the Web," technical report, Stanford Digital Library Technologies Project.

[11] Erman Ayday, Student Member, IEEE, and Faramarz Fekri, Senior Member, IEEE "Iterative Trust and Reputation Management Using Belief Propagation" IEEE Transactions on dependable and secure computing, Vol. 9, No. 3, May/June 2012

[12] S. Buchegger and J. Boudec, "Coping with False Accusations in Misbehavior Reputation Systems for Mobile Ad Hoc Networks," Technical Report IC/2003/31, EPFL-DI-ICA, 2003.

[13] A. Whitby, A. Josang, and J. Indulska, "Filtering Out Unfair Ratings in Bayesian Reputation Systems," Proc. Seventh Int'l Workshop Trust in Agent Societies (AAMAS '04), 2004.

[14] D. Clarke, J Elien, C. Ellison, M Fredette, A Morcos, and R.L. Rivest, "Certificate Chain Discovery in SPKI/SDSI", Journal of Computer Security, Vol. 9, No.4 ,2001, pp.285-322. Proc. Of the IEEE Symposium om security and Privacy, My 2002, pp.114-130.

[15] M. Blaze, J. Feigenbaum, and J. Lacy,"Decentralized trust management", IEEE Symp on Security and privacy, May 1996, pp.164-173.

[16] Amit Mathur, Suneuy Kim, Mark Stamp, "Role based access control and JXTA peer-to-peer Framework" www.truststc.org,2005

[17] Kui MENG, Xu ZHANG, Xiao-chun XIAO, Geng-du ZHANG "A Bi-rating Based Personalized Trust Management Model for Virtual Communities" 1-4244-0065-1/06/$20.00 2006 IEEE

[18] Wenjing Cui, Haiyang Wang, Qi Sui, Lizhen Cui, School of Computer Science and Technology, Shandong University, China "Towards a Trust Management Model for E-travel" 1-4244-0963-2/07/$25.00 ©2007 IEEE.

[19] Jianli Hu1, Xiaohua Li, Bin Zhou, Yonghua Li, "A Reputation Based Attack Resistant Distributed Trust Management Model in P2P Networks", 2010 Third International Symposium on Electronic Commerce and Security

[20] *Hui Xia, Zhiping Jia *, Xin Li, Feng Zhang* School of Computer Science and Technology Shandong University Jinan, P.R. China "*A Subjective Trust Management Model based on AHP for MANETs*", 2011 International Conference on Network Computing and Information Security

[21] Ryma Abassi , Sihem Guemara El Fatmi, Higher School of Communication, Sup'Com University of Carthage Tunis, Tunisia" Towards A Genric Trust Management Model" , 19th International Conference on Telecommunications (ICT 2012), 978-1-4673-0747-5/12/$31.00 ©2012 IEEE

[22] Xiaodong Sun School of Information Science and Engineering Northeastern University Guiran Chang, Fengyun Li school of Information Science and Engineering Northeastern University Shenyang, P. R. China, "A Trust Management Model to enhance security of Cloud Computing Environments", 2011 Second International Conference on Networking and Distributed Computing, 978-0-7695-4427-4/11 $26.00 © 2011 IEEE

[23] Thomas Beth, Malte Borcherding & Birgit Klein, Valuation of Trust in Open Networks, *ESORICS 94*, Nov 1994.