Trust Establishment in Ad Hoc and Sensor Networks

Efthimia Aivaloglou, Stefanos Gritzalis, and Charalabos Skianis

Information and Communication Systems Security Laboratory,
Department of Information and Communication Systems Engineering,
University of the Aegean, Samos, Greece
{eaiv,sgritz,cskianis}@aegean.gr

Abstract. Ad hoc and sensor networks highly depend on the distributed cooperation among network nodes. Trust establishment frameworks provide the means for representing, evaluating, maintaining and distributing trust within the network, and serve as the basis for higher level security services. This paper provides a state-of-the-art review of trust establishment frameworks for ad hoc and sensor networks. Certain types of frameworks are identified, such as behavior-based and certificate-based, according to their scope, purpose and admissible types of evidence. Moreover, hierarchical and distributed frameworks are discussed, based on the type of ad hoc and sensor networks they are designed for. The review is complemented by a comparative study built both on criteria specific to each category and on common criteria, grouped into three distinct classes: supported trust characteristics, complexity and requirements, and deployment complexity and flexibility.

Keywords: Trust establishment, trust evaluation, ad hoc networks, sensor networks.

1 Introduction

Mobile ad hoc networks are temporary wireless networks, formed dynamically by a set of mobile nodes without relying on any central infrastructure. Ad hoc networks are characterised by randomly changing topologies, distributed control and cooperative behaviour. Sensor networks, as a special case of ad hoc networks, are composed of inexpensive, small and resource constrained sensor nodes, densely spread over sensing fields. The distributed and dynamic nature of these types of networks are highly desirable properties when considering the design of security solutions for Critical Information Infrastructures (CIIs). CIIs, offering information and communication services which are significantly affecting quality of life, safety, and economic activities, may thus include ad hoc and sensor network technologies not only for the provision of context-rich services, but also for their protection in crisis situations.

The design of secure ad hoc and sensor networks is an active research area. Securing ad hoc and sensor networks generally entails ensuring the confidentiality

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 179–194, 2006.

and integrity of the data communicated, providing the means for node authentication and access control, along with lower level security issues like secure routing and node grouping. However, several works (e.g., [1,2,3,4]) argue that the conventional view of security does not suffice provided the unique characteristics of ad hoc networks, that are susceptible to a variety of node misbehaviours. From compromised nodes acting as internal attackers to legitimate nodes that act selfishly or maliciously, internal misbehaving nodes are a vulnerability that can not be tackled using authentication and cryptography alone. This vulnerability, along with the cooperative nature of ad hoc and sensor networks, rise the necessity for assessing the trust relationships among the network nodes. The trust relationships established between network nodes could be used for the provision of higher level security solutions, such as trusted key exchange or secure routing. However, the trust evaluation requirements and challenges posed by ad hoc networks are substantially different from the case of traditional wired networks. The existence of trusted third parties used as intermediaries for establishing trust relationships cannot be taken for granted, trust relationships change frequently due to the dynamic topology, while trust evaluation may be based on uncertain and incomplete evidence due to connectivity problems. To tackle the aforementioned new challenges, trust establishment frameworks have been proposed for representing, evaluating, maintaining and distributing trust among ad hoc network nodes.

The rest of the paper is organised as follows: Section 2 discusses the notion of trust in ad hoc and sensor networks and the challenges and requirements related to trust establishment. Section 3 presents a selection of the trust establishment frameworks, separated into two categories according to their scope and purpose, and compared according to criteria specific to each category. Section 4 contains the comparative evaluation on issues that are common for all frameworks presented, and discusses issues related to the applicability on sensor networks. Finally, Section 5 concludes the paper and suggests future directions.

2 The Notion of Trust in Ad Hoc Networks

The notion of trust, as used in different research areas like trusted computing, trusted platforms, trusted code and trust management, has received various interpretations [5]. Throughout this work, we study the in-network trust relationships that can exist between network entities. We use the notion of trust as "The quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context" [6]. A trust relationship is established by two parties, the trustor and the trustee, also referred to in this work as the trust issuer and the target. The *trust establishment* process includes the specification of valid types of evidence, and its generation, distribution, collection and evaluation [7].

Trust evidence, which form the basis for establishing trust relations, may be uncertain, incomplete, stable and long-term [8]. *Trust evaluation* is performed by applying context-specific rules, metrics and policies on the trust evidence. The result of the process is the *trust relation* between the trustor and the trustee, usually represented as a certificate or as a numeric value, either discrete or in a continuous range. Trust relations can be *revoked* on the basis of newly obtained evidence. Trust is *transitive* if it can be extended beyond the two parties between whom it was established, allowing for the building-up of trust paths between entities that have not directly participated in a process of trust evaluation. In general, the problem of formulating evaluation rules and policies, representing trust evidence, and evaluating and managing trust relationships is referred to as the *trust management* problem [9].

Provided that ad hoc networks highly depend on the distributed cooperation among network nodes, while being susceptible at the same time to node misbehaviour, the formation of trust relationships within the network could serve as the basis for higher level security solutions. However, the inherent properties of ad hoc and sensor networks both at node and network level pose challenges unique for the trust management area. Ad hoc, and especially sensor nodes, have constrained energy, memory, computation and communication capabilities. The wireless nature of communications, the dynamically changing topology and membership, and the lack of fixed infrastructure are also parameters that affect the design of trust evaluation frameworks for ad hoc and sensor networks. The lack of centralised monitoring and management points preclude the use of trusted intermediaries, such as trusted third parties or certification authorities (CAs) for trust establishment. Each node needs to manage trust relationships with other nodes individually. Due to the vulnerability of wireless links and the frequent topology changes, connectivity can not be assured, and thus stable hierarchies of trust relations can not be supported. Moreover, because of the varying connectivity and the dynamic topology, trust establishment needs to support evidence that may be uncertain and incomplete, since it can only be sporadically collected and exchanged for each node under evaluation [7,8].

The susceptibility to node misbehaviour can affect not only network operations, but also the trust evaluation framework itself. Especially for frameworks that require cooperative trust evaluation, it is crucial that the nodes are willing to cooperate by making recommendations or evidence that they may hold for the target node available. However, this is not the case in ad hoc networks, since nodes may behave selfishly to preserve resources. Malicious nodes may also perform bad mouthing attacks against legitimate nodes to spread bad reputation, either by directly spreading false evidence or by pretending to be victims of mad mouthing themselves to make a legitimate node look malicious [10].

An additional requirement that mainly applies to sensor networks, is that pre-established and stable trust relationships must be supported. Some sensor nodes may be clustered by deployment so that trust relationships within the cluster may be assumed long-term and stable. For body sensor networks, for example, it is unlikely that a node may misbehave or be compromised. Within such predefined clusters, trust relationships do not need to be continuously evaluated.

As a result, trust establishment protocols for ad hoc and sensor networks should:

- Be decentralised, not based on on-line trusted parties. Instead, they should support distributed, cooperative evaluation, based on uncertain evidence.
- Support trust revocation in a controlled manner.
- Scale to large deployments and be flexible to membership changes.
- Entail acceptable resource consumption, especially for sensor networks.

3 Trust Establishment Frameworks for Ad Hoc Networks

The trust establishment frameworks proposed for ad hoc and sensor networks can be classified into two categories according to their scope, purpose and type of evidence that trust evaluation is based on.

Certificate-based frameworks aim to define mechanisms for pre-deployment knowledge on the trust relationships within the network, usually represented by certificates, to be spread, maintained and managed either independantly or cooperatively by the nodes. Trust decisions are mainly based on the provision of a valid certificate, that proves that the target node is considered trusted either by a certification authority or by other nodes that the issuer trusts. It is generally outside the scope of certificate-based frameworks to evaluate the behaviour of nodes and base trust decisions on that evaluation.

In behavior-based frameworks, each node performs trust evaluation based on continuous monitoring of the behavior of its neighbors, in order to evaluate how cooperative they are. Although a mechanism that determines the identities of the nodes is usually assumed to exist, it is generally outside the scope of behavior-based trust establishment models to securely authenticate other nodes and to determine whether they are legitimate members of the network. In that sense, behavior-based models are more reactive than certificate-based models. As an example, if a node makes unauthorised use of the network and behaves selfishly or maliciously, it will not manage to gain or retain a trust level that will allow it to cooperate with other nodes, and it will be thus isolated.

Alternatively, the frameworks are characterised as hierarchical or distributed, according to the type of ad hoc or sensor networks they were designed for. Hierarchical frameworks assume the existence of a hierarchy among the nodes, based on their capabilities or level of trust. These frameworks may specify, for example, that certification authorities or trusted third parties provide on-line or off-line evidence. Distributed frameworks assume that there is no fixed infrastructure, and the responsibility of acquiring, maintaining and spreading trust evidence is equally spread among the network nodes. This distinction mainly applies for certificate-based frameworks, since the behavior-based are all designed for distributed networks.

3.1 Certificate-Based Trust Establishment

The most widely used approach for certificate-based trust establishment is the traditional, hierarchical, public key infrastructure model formed as an organisation of certification authorities. The use of on-line certification authorities for ad hoc networks, however, is problematic for connectivity and service availability reasons. Three generic approaches for certificate-based trust establishment have been proposed, two of which are hierarchical and one is distributed. In the first hierarchical approach, trust is represented by certificates signed by offline trusted third parties, whose public keys the trustors need to possess to verify the signatures. The second is a fully distributed self-organised public key management scheme, where trust is evaluated using certificate chains. The third one utilises secret sharing mechanisms to distribute trust to an aggregation of nodes that can collaboratively provide certification authority services. This is considered to be a hierarchical approach, since trust is distributed among a subset of network nodes, that are designated to represent a certification authority.

Hierarchical Trust Frameworks. A hierarchical progressive trust negotiation scheme for ad hoc networks is introduced by Verma et al. [11]. Off-line trusted third parties are set responsible both for issuing the certificates required for each node, including a network address certificate and at least one identity certificate, and for issuing certificate revocation lists. The model includes the notion of certificate release policies that are used to enforce a negotiating strategy for each node, in order for the disclosure of information to be controlled during trust negotiation. Each node in the network stores the certificates of the third parties and the certificate revocation lists they have issued, along with the local certificates to be used in trust negotiation. Trust negotiation is carried out by incrementally exchanging certificates.

In [12], Davis proposes a scheme that similarly uses certificates based on a hierarchical trust model to manage trust, and also enables explicit revocation of certificates without input from trusted third parties. The only task in the scheme that is not performed locally at each node is the issuing of certificates. Any node j is considered trusted by any node i once it presents a certificate that has not expired, has not been revoked, and i can verify using the public key of a third party. Nodes have to maintain locally their private keys and the public keys of the third parties.

To handle certificate revocation without input from third parties, nodes maintain certificate status tables and profile tables that contain information about the behaviour profile of each node in a network, which is used to determine whether or not a given certificate should be revoked. The profile tables kept by all nodes in the network should be consistent. In case inconsistencies are found by any node, accusations are broadcasted for the nodes that sent the inconsistent data. The two tables of all nodes are updated when an accusation is broadcasted, thus the accused node's certificate is revoked and network access is denied. In order to defend against bad mouthing attacks, the authors propose the final decision on certificate revocation to be based on a sum of weighted accusations from independent nodes.

Distributed Trust Frameworks. In contrast to the hierarchical frameworks, where certificates are issued by trusted third parties, distributed frameworks provide mechanisms for trust evaluation between network nodes in a cooperative, self-organised manner. The Pretty Good Privacy model (PGP) [13] was the first to enable users to act as independent certification authorities, expressing their trust on other users (the confidence on their identity) by validating their public keys. The public key certificates of this so-called "web of trust" approach are assigned with trust levels and confidence levels. However, although certificates are issued by the users, publicly accessible certificate directories are required for their distribution, which makes the model inapplicable for ad hoc networks.

A framework that uses the "web of trust" approach of the PGP model, without requiring certificate directories for the distribution of certificates, is proposed by Hubaux et al. [14]. The relationships between users are modeled as a directed graph, called trust graph, whose edges represent public key certificates. Each user maintains a subset of the trust graph as a local repository of certificates issued by himself or other users in the system. A subgraph selection algorithm is proposed, which is called Shortcut Hunter Algorithm. When a user i wants to obtain the public key of user j, they merge their subsets of trust graph stored in their repositories and i tries to find a trust route in the form of a certificate chain from i to j in the merged repository.

To deal with dishonest users issuing false certificates, an authentication metric is introduced as a function that takes two users i and j and a trust graph as inputs and returns a value that represents the assurance with which i can obtain the authentic public key of j using the trust graph. In the general case, however, it is assumed that the requester nodes trust the nodes in the generated certificate chains. Moreover, it is considered that this framework is practically inapplicable for ad hoc networks because it requires extensive public-key operations for constructing certificate chains [15,3].

The distributed trust establishment framework proposed by Eschenauer et al. [8] takes a broader view on the inputs required for node trust decisions by accepting as trust evidence not only certificates and public keys, but also information like identities, locations, or independent security assessments. The type of information required depends on the policy and the evaluation metric each node uses to establish trust. Trust metrics are used to assign confidence values to available pieces of evidence that may be uncertain or incomplete, while policy decisions are defined as a local procedures that, based on the evidence and the confidence assigned to it, output a trust decision.

The framework is fully distributed. Any node can generate trust evidence about any other node and make it available to others through the network, as long as it signs it with its private key and specifies its lifetime. The evidence is then replicated within the network to ensure availability. Evidence revocation is supported through revocation certificates and by the generation and distribution of contradictory evidence. To protect against bad mouthing attacks, when evidence revocation occurs, it is proposed that the policy decisions require redundant pieces of evidence from independent sources to proceed to the evaluation.

Distributed Certification Authority Frameworks. The use of secret sharing to distribute the CA functionality among a set of nodes in ad hoc networks was first proposed by Zhou and Haas [16]. Their Distributed Public Key Model takes advantage of redundancies in the network topology to achieve availability of the CA service, that is provided by an aggregation of nodes that trust is distributed to. The model uses threshold cryptography to distribute the private key of the CA over a number of network nodes n, that share the ability to perform cryptographic operations. The scheme allows for any $t+1$ out of n nodes to combine their partial keys to collaboratively generate the secret key of the service and sign certificates, whereas this would be unfeasible for any t nodes.

For an adversary to acquire the secret key, at least $t+1$ of the designated nodes must be compromised. In order to tolerate mobile adversaries, the authors make their threshold cryptography scheme proactive by using share refreshing. This enables the designated nodes to derive new partial keys from the old ones in collaboration, without having service secret key disclosed to any of them.

The Mobile Certificate Authority framework, presented by Yi and Kravets [17], similarly uses threshold cryptography to distribute trust. Provided that heterogeneity is expected to exist among ad hoc network nodes, the nodes that are assigned with CA functionality, called MOCAs, are selected according to criteria like computational power, physical security or risk of compromise. The framework includes a communication protocol that client nodes are equipped with in order to correspond with MOCAs for certification services, by contacting at least $t+1$ MOCAs and receiving at least $t+1$ replies.

The framework deals with trust revocation through certificate revocation lists, stored at each node, at the MOCAs, or at a set of specially designated nodes. For a certificate to be revoked, each MOCA signs a revocation certificate with its partial key and broadcasts it. When revocation certificates are gathered from least $t+1$ MOCAs, the certificate revocation list is updated. Bad mouthing attacks could thus only be successful if $t+1$ MOCAs are compromised.

Summary and Remarks. The PGP-like distributed trust frameworks are considered to offer more flexibility than the hierarchical frameworks, but may not be suitable for applications where high degrees of accountability and security are required [12]. The main reasons are that they are less structured and more prone to attacks by malicious agents, since it does not have any central management point like a CA, enforcing strict policies on trust assessment.

The Distributed Certification Authority Frameworks are considered are quite robust, but are the ones that impose the greater deployment complexity and have the higher communication requirements per evaluation request. Moreover, it is considered that threshold cryptography is too computationally expensive to be used in ad hoc networks. Finally, these frameworks require cooperation of ad hoc network nodes that may behave selfishly to preserve resources [14,12]. For these reasons, the applicability of secret sharing schemes in ad hoc networks is considered limited.

3.2 Behaviour-Based Trust Establishment

The behaviour-based trust models view trust as the level of positive cooperation between neighboring nodes in a network. Trust is evaluated both independently

Table 1. Characteristics of Certificate-Based Trust Frameworks. For each framework, the *type of evidence* that is required for trust evaluation of node j by node i is caterised as: (C/PK)-Certificate/Public Key, (RI)-Trust Revocation Information like Certificate Revocation Lists (CRLs) or similar structures, (CD)-Context-Dependent information like location, identity, etc., (CF)-Confidence Factor on Evidence/Recommendations, (TD)-Time-Dependency of Evidence or Recommendations. The *evidence provision* column presents the input required by the evaluation mechanism performed by i from each of the parties involved in the evaluation. The *pre-configuration* column includes the information each node x in the network must posses before entering the network. The representations used are: (K_x)-Private key of node x. (C_x^y)-Certificate issued for x by y. A represents the certification authority. The set N represents all nodes in the network.

Trust	Required Evidence					Parties Involved	Evidence Provision	Pre-Configuration
Framework	C/PK	RI	CD	CF	TD			
Hierarchical Trust Frameworks								
[11]	+	+				i,j,n CAs	i:C_A^A&n CRLs, j:C_j^A	C_x^A,K_x,nC_A^As
[12]	+	+				i,j,n offline CAs	i:C_A^A&RI, j:C_j^A	C_x^A,K_x,nC_A^As
Distributed Trust Frameworks								
[14]	+					i,j	i:REP_i,j:REP_j	K_x, REP_x:$nC_{y\in N}^{z\in N}$s
[8]	+	+	+	+	+	i,j, any other	j, any other	Keys, Policy, Metrics
Distributed Certification Authority Frameworks								
[16]	+					i,j,$t+1$ partial CAs	i:C_A^A, CAs:C_j^A	x:K_x, CAs:$K_{t\in CAs}^{partial}$
[17]	+	+				i,j,$t+1$ partial CAs	i:C_A^A&RI, CAs:C_j^A	x:K_x, CAs:$K_{t\in CAs}^{partial}$

by each node based on observations and statistical data that is being continuously accumulated by monitoring the network traffic, and cooperatively through sharing recommendations and spreading reputation. The basic aim of these behaviour-based models is to isolate the nodes that either act maliciously because they have been compromised, or selfishly in order for example to preserve resources, by assigning and recommending low levels of trust.

The result of the independent evaluation is called *direct trust*, since it is based on the direct experience the trustor node may have on the trustee node. There have been several works on monitoring the behaviour of neighboring nodes in ad hoc networks, such as intrusion detection systems (a survey can be found in [18]), from which many aspects are borrowed by the behaviour-based frameworks. The evidence collection mechanisms are usually placed below the application layer, in order to evaluate routing behaviours and information integrity. In the context of sensor networks, even the raw data communicated could be evaluated for consistency among neighboring nodes [1]. What should be noted however is that monitoring the network traffic is very resource consuming, in terms of computation, memory and energy. For example, the radio on each node needs to be continuously enabled, while the trust values of all neighboring nodes need to be stored and continuously updated as interactions occur.

Indirect trust is derived using recommendations from other nodes, which usually are their trust values for the target node. Selection criteria may be applied for the neighboring nodes that will provide the recommendations [2]. The indirect trust derivation process may include weighting the recommendations of other nodes based on how trusted they are [7,1,2], or providing confidence values along with the recommendations [7]. The result of the recommendations exchange for computing indirect trust is that node reputation is spread through the network, enabling the formation of a connected trust graph. The most important factor that could hinder this process is node selfishness and unwillingness to spread reputation information. Including node cooperation on reputation spreading for the calculation of direct trust is one of the countermeasures.

The functions that are specified in most behaviour-based trust frameworks in order to evaluate the trust value of the trustor network node i to the trustee network node j are:

- A function $DT(i, j)$ for calculating the direct trust value, based on previous interactions and network traffic monitoring metrics. This function is considered implementation dependent and, as such, it is not explicitly defined in the trust evaluation frameworks that are studied.
- A function $IDT(i, j)$ for calculating the indirect trust value based on recommendations from neighboring nodes.
- A function $T(i, j)$ for calculating the final trust decision through balancing the relationship between direct and indirect trust. The result of this calculation is compared against a trust threshold to reach the final decision on node cooperation. Frameworks like [4] also include context and action specific metrics for computing T.

The factors being used by the trust frameworks in this section regarding the computation of the direct and indirect trust and the final decision are enlisted in Table 2. The symbols representing the factors in the table are also being used for the representation of the trust evaluation functions. For uniformity reasons, the functions presented in the following paragraphs use a set of symbols that are different from those used on the original forms.

Behaviour-Based Frameworks. Yan et al. [4] proposed one of the first behaviour-based trust evaluation frameworks for ad hoc networks. It defines a trust evaluation matrix for each network node to store the knowledge derived through both network traffic monitoring and recommendations. While the framework does not include functions for direct trust computation or indirect trust combination, it proposes a linear function that computes the trust value for an action a based on the evaluation parameters in the trust matrix and the preferences of the trustor node. The preferences are expressed as factor rates $r_x(i, j, a), x \in \{NTM, R, CAd, CAo\}$, each used for weighting a factor as expressed in Table 2. Factors CAd and CAo represent the importance of the communication data and other parameters like energy left, frequency of routing request, etc. Trust of node i to node j for an action a is evaluated as:

$$\begin{aligned} T_a(i, j) = [&r_{NTM}(i, j, a) * DT(i, j) + r_{CAd}(i, j, a) * V_{CAd}(i, j) \\ &+ r_R(i, j, a) * IDT(i, j) + r_{CAo}(i, j, a) * V_{CAo}(i, j)] * V_{BL}(i, j) \end{aligned} \qquad (1)$$

Functions $V_x(i, j), x \in \{CAd, CAo, BL\}$ are the functions that evaluate the corresponding factors. Function $V_{BL}(i, j)$ returns a value in (1,0) of the intrusion detection black list, thus enforcing zero trust level for the nodes included in it.

Table 2. Evaluation Parameters of Behaviour-Based Trust Frameworks. Parameters are: (NTM)-Network Traffic Monitoring, (WCE)-Weighted Combination On Event Significance, (WFE)-Freshness as as Weight Factor for the Events, (BL)-Black Lists, (R)-Recommendations From Neighboring Nodes, (RCF)-Confidence Factor on Recommendations, (WCR)-Weighted Combination of Recommendations, (WCDI)-Weighted Combination of DT - IDT, and (CA)-Context and Action Specific Metrics like value of data, energy left, QoS, etc.

	Direct Trust Evaluation				Indirect Trust Evaluation			Comb. & Final Decision	
Trust Framework	NTM	WCE	WFE	BL	R	RCF	WCR	WCDI	CA
[4]	+			+	+			+	+
[3]	+	+							
[7]	+				+	+	+		
[1]	+		+		+		+		
[2]	+				+		+	+	

A trust model for finding trustworthy routes in ad hoc networks that is entirely based on direct trust evaluation is proposed by Pirzada and McDonald [3]. In their model, they make use of independent trust agents that reside on network nodes, each one gathering network traffic information in passive mode by applying appropriate taps at different protocol layers. The information gathered from these events is classified into trust categories, so that the *situational trust* $TS(i, j, x)$ for node j can be computed using the information of trust category x. Moreover, weights $W_i(x)$ are assigned according to the utility and importance of each trust category to i. The general trust is thus computed as the trust that the trustor node i assigns to the trustee node j based upon all previous transactions in all situations, according to their significance:

$$T(i,j) = DT(i,j) = \sum_{x=1}^{n} [W_i(x) * TS(i,j,x)] \qquad (2)$$

A different view on trust evaluation is proposed by Theodorakopoulos and Baras [7], who mainly focus on the evaluation of indirect trust as the combination of opinions from neighboring nodes, assuming that some mechanism exists for these nodes to assign their opinions based on local observations. The process of indirect trust evaluation is formulated as a shortest path problem on a weighted directed graph, where graph nodes represent network nodes and edges represent trust relations. The edges are weighted with the trust value the issuer node has on the target node and the confidence value it assigns on its opinion, depending on the number of the previous interactions and positive direct evaluations. The theory of semirings is being used for formalising two versions of the trust inference problem: finding the trust-confidence value that node i should assign to node j, based on the trust-confidence values of the intermediate nodes, and finding a sequence of nodes that has the highest aggregate trust value among all trust paths from i to j. The authors define path and distance seminarings for computing the trust distance along trust paths from the issuer to the target, and a computation algorithm that is an an extension to Dijkstra's algorithm.

Ganeriwal and Srivastava [1] propose a different framework for the evaluation of indirect trust, that is designed for wireless sensor networks. The Reputation-based Framework for Sensor Networks (RFSN) includes a watchdog mechanism for monitoring the behaviour of neighboring nodes in terms of data forwarding and raw sensing data consistency. Each sensor node maintains reputation for other nodes in the form of a probabilistic distribution, and trust is obtained by taking its statistical expectation. Reputation $R_{i,j}$ is built based on the results of the watchdog mechanism (direct reputation) in combination with second hand information for deriving the indirect reputation $IDR_{i,j}$. The following equation is defined for computing the indirect reputation by weighting the second-hand information from the neighboring nodes of i, denoted as N_i:

$$IDR_{i,j} = IDR_{i,j} + \{g(R_{i,k}) * R_{k,j}\} \forall k \in N_i \tag{3}$$

Within the framework of RFSN, the authors propose an example system based on a Bayesian formulation for representing reputation and trust evolution. What is of special interest is the incorporation of exponential averaging when combining reputation information in order to place more weight on recently obtained information. Moreover, they propose propagation of good reputation information only to protect against bad mouthing attacks. In order to discourage adversaries from changing identities or creating virtual nodes, the initial reputation of each node is a null value and has to be gradually built.

Huang et al. [19] developed a similar trust evaluation model, one extension of which is the requirement for an authentication mechanism to ensure that all identities are trustworthy. Except from the Bayesian formulation, the authors also propose the Dempster-Shafer Theory of Evidence for combining evaluations.

A Trust-Domain based security architecture for mobile ad-hoc networks is proposed by Virendra et al. [2]. It includes a behaviour-based trust evaluation framework that is used both as the basis for key establishment decisions and for secure node grouping that can enable distributed control in the network. Trust evaluation is based both on direct and indirect knowledge. For computing direct trust, network monitoring parameters related to traffic volumes and information integrity are listed and a traffic statistics function is presented but not precisely defined. Four schemes are proposed for combining indirect trust information, the most sophisticated of which is is the double weighted approach:

$$IDT(i,j) = \frac{\sum_{k \in O} T(k,j) / \sum_{m \in O} T(m,j) * T(i,k)}{\sum_{k \in O} T(i,k)} \tag{4}$$

The set O appearing in the equation is the set of nodes in the range of both i and j, that i trusts above a certain threshold. Function $T(i,j)$ for calculating the final trust decision balances the relationship between direct and indirect trust through utilising weighting factors.

Summary and Remarks. It can be observed from the frameworks presented above that, several formalizations of different complexity have been proposed, from weighted average to the use of probabilistic distributions and semirings, for the most interesting function in trust evaluation, the one for calculating the indirect trust value based on recommendations. The exchange of recommendations enables the view of the network as a connected trust graph, where trust is gradually built for each node through good reputation, but also gradually revoked as a result of malicious behaviour. In the presence of intrusion detection mechanisms issuing black lists, only the framework proposed by Yan et al. [4] enables immediate trust revocation. It is also noted that none of the frameworks supports pre-established and stable trust relationships, since they do not include any bias with respect to the identity of the node under evaluation.

4 Comparative Evaluation

The comparison of the trust establishment frameworks that were presented in the previous sections is based on the following three criteria: The characteristics of trust that each framework supports, the complexity and resource requirements it would impose, and its deployment complexity and flexibility. The applicability of each framework in sensor networks is separately discussed. Emphasis here is given on common issues for behavior-based and certificate-based frameworks, since those that are specific for each category are already discussed at the corresponding sections. Table 3 presents the evaluation of each framework for the following categories of criteria:

Supported Trust Characteristics include support for uncertain evidence, transitivity of trust and trust revocation. The use of uncertain evidence is characterised as controlled for frameworks that support assignment of confidence values to evidence supplied for trust evaluation, including recommendations from other nodes. Transitivity of trust, if supported, is considered controlled if trust values from third parties are weighted according to the trust relationship the requester has with the third party, before being used for trust evaluation. For frameworks that support trust revocation, it is considered controlled if either trust is revoked only by trusted third parties or some mechanism exists to protect from bad mouthing attacks. Moreover, trust revocation is characterised gradual if trust is not revoked explicitly, but as the result of bad reputation spread gradually due to node misbehaviour.

Complexity and Requirements in memory, computational power and communications. Due to the lack of homogeneity among the frameworks in the data structures used as evidence, the algorithms and functions used as primitives for trust evaluation, and the communication patterns during the trust establishment process, the evaluation on these criteria is somewhat subjective. It is considered that a model has high memory requirements if each node needs to store information about every other node in the network, or maintain detailed information about previous interactions and events. High computational power would be required to perform frequent public key operations, or for continuously monitoring surrounding nodes and re-evaluating trust relationships based on every event monitored. Communication requirements increase the more messages need to be exchanged between the interested nodes or third parties for a trust relationship to be established or revoked, and the more broadcasts that are required, either for trust revocation or for initialisation when a new node enters the network.

Table 3. Comparative Analysis of Trust Establishment Frameworks for Ad Hoc Networks The evaluation criteria are: (UC)-Uncertainty of Evidence, (TR)-Trust Transitivity, (RC)-Trust Revocation, (MEM)-Memory Requirements, (CMP)-Computational Complexity, (CMN)-Communication Requirements, (PC)-Pre-Configuration Required, (SE)-Scalability and Extensibility. The values are: (C)-Controlled, (U)-Uncontrolled, (N)-Not Supported, (G)-Gradual, (I)-Immediate, (H)-High, (M)-Medium, (L)-Low.

Trust	Supported Trust Characteristics			Complexity and Requirements			Deployment Issues	
Framework	UC	TR	RC	MEM	CMP	CMN	PC	SE
Certificate-Based Trust Frameworks								
[11]	U	N	C, I	M	M	H	M	H
[12]	U	N	C, I	H	H	H	M	M
[14]	U	U	N	M	H	M	M	M
[8]	C	C	C, I	M	M	M	H	H
[16]	U	N	N	M	H	H	H	H
[17]	U	N	C, I	H	H	H	H	H
Behaviour-Based Trust Frameworks								
[4]	U	U	U, G/I	M	M	M	M	M
[3]	U	N	U, G	M	L	L	L	H
[7]	C	C	U, G	L	M	M	L	M
[1]	U	C	C, G	L	M	M	L	M
[2]	U	C	U, G	H	M	M	L	H

Deployment Issues include pre-configuration, scalability and extensibility issues. The amount and complexity of the required pre-configuration is characterised as high when detailed trust policies and metrics need to be defined for each node, or when the keying material each node needs to be supplied with requires special selection or generation algorithms. Scalability and extensibility decisions are based on how the model would scale on large deployments, and how easily new nodes could be added. For example, low scalability and extensibility is assigned for models that require each node to maintain information for all other nodes, and update it every time a new node enters and broadcasts its information.

An issue that is not included in Table 3 is the additional *battery power consumption* the application of each model would impose to ad hoc network deployments. The issues included in the complexity and requirements category affect the energy requirements in different degrees. However, although behaviour-based trust evaluation models appear less complex, they would probably be more energy consuming because they require nodes to keep their radio constantly on in order to monitor their neighbors.

Concerning the *representation of trust*, none of the frameworks uses discrete values, since it is considered too restrictive. Behaviour-based evaluation frameworks represent trust in a continuous range and compare its value with a trust threshold to decide on node cooperation. Certificate-based frameworks base the decision on node cooperation on the provision of a trusted certificate, i.e. a certificate that either is valid since it is signed by a (distributed or centralised) trusted third party, or a trusted certificate chain that includes it can be formulated.

None of the behaviour-based models supports *pre-established and stable trust relationships.* From the certificate-based frameworks, pre-established trust could be supported by [8] through introducing identity related bias in the trust metrics and policies of the nodes. For the framework introduced by Hubaux et al. [14], this requirement could be satisfied if the certificate repositories of nodes were configured to include the certificates of trusted nodes that each issuer should maintain direct and stable trust relationships with.

The issue of tackling *node selfishness*, that is especially important for frameworks that entail node cooperation, either for reputation spreading or for providing CA functionality, is not sufficiently addressed in the frameworks studied. In the model proposed by Weimerskirch and Thonet [15], incentives and punishment mechanisms are specified for recommendating nodes.

Applicability on Sensor Networks. The main issues that need to be taken into account for assessing the applicability of the presented frameworks on sensor networks are related to their complexity and resource requirements. As explained in Sect. 2, sensor nodes are severely constrained regarding their energy, memory, computation and communication capabilities. Behaviour-based trust evaluation frameworks utilize techniques similar to the ones of intrusion detection schemes, which are considered expensive in terms of memory, energy and communications requirements [20]. Both the need for nodes to keep their radio constantly on in order to monitor their neighbors, and the need for continuous evaluation of their trust values, are unrealistic for the constrained sensor nodes.

The same constraints in memory and computational capabilities pose concerns on the applicability of the certificate-based trust frameworks, that utilise asymmetric cryptography. Traditional asymmetric cryptography is considered too expensive for sensor nodes [10,21]. However, Elliptic Curve Cryptography, that has recently emerged as an attractive alternative to traditional public key generation, is considered to be efficient enough to be attained and executed on resource-constrained sensor nodes, mainly due to the fact that it can offer equivalent security with smaller key sizes [21].

It is our belief, however, that both the behaviour-based and the certificate-based frameworks compared are better targeted for ad hoc than for sensor networks. The main reasons are that they do not exploit the pre-deployment knowledge that will usually be available in sensor network deployments, and they do not allow for pre-established, stable trust relationships. A possible way for the trust establishment frameworks to be applied in sensor networks is by using the intrusion detection systems paradigm: as services by a subset of the nodes, e.g. the cluster heads, so as not to consume the resources of the entire network.

5 Conclusions

The discussion on the behaviour-based and certificate-based trust establishment frameworks and their comparison both in common and in category-specific criteria has highlighted the different approaches taken in the representation and evaluation of trust, and their pros and cons in terms of complexity, requirements and scalability. The differences in scope and purpose between the two categories of frameworks show that they should not be viewed as alternative approaches, but as supplementary. It would be possible, for deployments that require high levels of accountability ans security, to combine a certificate-based with a behaviour-based trust framework to benefit both from the representation of pre-deployment trust relationships as certificates and from the continuous behaviour-based evaluation of trust.

What the comparison has also shown, however, is that the more sophisticated a trust establishment framework is in terms of supported trust characteristics and resilience to node compromise, the more complex and resource consuming it becomes. The computational complexity of the certificate-based and the energy requirements of the behaviour-based trust evaluation frameworks raise concerns related to their applicability on resource constrained sensor nodes. At the same time, none of the frameworks studied aims to fulfill the special requirements of sensor networks on the representation and evaluation of trust relationships. In the future, it would be interesting to see less complex frameworks, especially targeted for sensor node relationships.

References

1. Ganeriwal, S., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN'04), ACM Press (2004) 66–77
2. Virendra, M., Jadliwala, M., Chandrasekaran, M., Upadhyaya, S.: Quantifying trust in mobile ad-hoc networks. In: IEEE International Conference on Integration of Knowledge Intensive Multi-Agent Systems (KIMAS'05). (2005) 65–71
3. Pirzada, A.A., McDonald, C.: Establishing trust in pure ad-hoc networks. In: Proceedings of the 27th conference on Australasian computer science (CRPIT'04), Australian Computer Society, Inc. (2004) 47–54
4. Yan, Z., Zhang, P., Virtanen, T.: Trust evaluation based security solution in ad hoc networks. In: Proceedings of the Seventh Nordic Workshop on Secure IT Systems. (2003)
5. Gollmann, D.: Why trust is bad for security. In: Electronic Notes in Theoretical Computer Science. Volume 157., Elsevier (2006) 3–9
6. Grandison, T.: Trust management for internet applications. PhD thesis, Department of Computing, University of London (2003)
7. Theodorakopoulos, G., Baras, J.S.: Trust evaluation in ad-hoc networks. In: Workshop on Wireless Security. (2004) 1–10
8. Eschenauer, L., Gligor, V.D., Baras, J.S.: On trust establishment in mobile ad-hoc networks. In: Security Protocols Workshop. (2002) 47–66
9. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: IEEE Symposium on Security and Privacy, IEEE Computer Society (1996) 164–173
10. Shi, E., Perrig, A.: Designing secure sensor networks. Wireless Communication Magazine **11**(6) (2004) 38– 43
11. Verma, R.R.S., O'Mahony, D., Tewari, H.: Ntm - progressive trust negotiation in ad hoc networks. In: Proceedings of the 1st Joint IEI/IEE Symposium on Telecommunications Systems Research. (2001)
12. Davis, C.R.: A localized trust management scheme for ad hoc networks. In: 3rd International Conference on Networking (ICN'04). (2004) 671–675

13. Garfinkel, S.: PGP : Pretty Good Privacy. OReilly & Associates (1995)
14. Hubaux, J.P., Buttyán, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, New York, NY, USA, ACM Press (2001) 146–155
15. Weimerskirch, A., Thonet, G.: A distributed light-weight authentication model for ad-hoc networks. In: Proceedings of the 4th International Conference Seoul on Information Security and Cryptology (ICISC'01), Springer-Verlag (2002) 341–354
16. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Network **13**(6) (1999) 24–30
17. Yi, S., Kravets, R.: Moca: Mobile certificate authority for wireless ad hoc networks. In: Proceedings of 2nd Annual PKI Research Workshop. (2003)
18. Djenouri, D., Khelladi, L., Badache, N.: A survey of security issues in mobile ad hoc and sensor networks. Communications Surveys & Tutorials, IEEE **7**(4) (2005) 2– 28
19. Huang, L., Li, L., Tan, Q.: Behavior-based trust in wireless sensor network. In: APWeb Workshops, Springer Berlin (2006) 214–223
20. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM **47**(6) (2004) 53–57
21. Arazi, B., Elhanany, I., Arazi, O., Qi, H.: Revisiting public-key cryptography for wireless sensor networks. IEEE Computer **38**(11) (2005) 103 – 105.