Quantitative Modeling of Trust and Trust Management Protocols in Next Generation Social Networks Based Wireless Mobile *Ad Hoc* Networks

Yogesh Malhotra, PhD, MSQF

December 14, 2014

Global Risk Management Network, LLC
Cornell Business and Technology Park
Ithaca, NY 14852-4892

Phone: (646) 770-7993 m, (646) 861-3680 v
e-mail: dr.yogesh.malhotra@gmail.com
http://www.linkedin.com/in/yogeshmalhotra

Quantitative Modeling of Trust and Trust Management Protocols in Next Generation Social Networks Based Wireless Mobile *Ad Hoc* Networks

Yogesh Malhotra

Abstract

Trust and Trust Management represent the very foundations of Computer and Network Security Protocols enabling all cyber activities. Recent spate of national and global high-impact Cyber Security compromises, threats, vulnerabilities, and exposures leads to fundamental questioning of *Trust* as the key enabler of all cyber phenomena in the unfolding era of exponentially increasing *Distrust*. It is therefore necessary to understand the current state of *Trust* and *Trust Management* modeling and implementation in the most high security environments such as in Defense & Space. Such understanding can serve as a foundation for modeling, design, and implementation of next generation mobile wireless networks for other high security environments such as in Banking & Finance. This study attempts to understand how Trust and Trust Management are being modeled for the "next generation wireless communication systems" (NIST) such as autonomous self-discovering, self-organizing, and self-adaptive *mobile ad hoc networks*. Within the context of Network-Centric Operations (NCO), we examine: (i) the capabilities of next generation wireless mobile ad hoc networks; (ii) how trust and trust management are modeled in such mobile ad hoc networks; and, (iii) how trust and trust management are implemented in trust-based task assignment in tactical networks. US Army Research Lab (ARL) Computational and Information Sciences Directorate's Network Science research program on wireless mobile ad hoc networks is the focus of our case study.

Keywords: Wireless Mobile Ad Hoc Networks, Network Security, Trust Management Protocols, Trust and Trust Management Modeling, Trust and Trust Management Metrics.

Words: 7,644

References & Notes: 41

Quantitative Modeling of Trust and Trust Management Protocols in Next Generation Social Networks Based Wireless Mobile *Ad Hoc* Networks

1. Introduction

As a preface to understand the modeling and implementation of trust and trust management for next-generation wireless communications systems, it will help to examine the overall context in which these issues are examined. Given our focus on high security environments, the specific Defense & Space context is that of next generation military tactical mobile wireless networks being designed by the US Army Research Lab's (ARL) Computational and Information Sciences Directorate. ARL situates the specific focus within its research on Network Science defined as [5]: "the study of complex systems whose behavior and responses are determined by exchanges and interactions between subsystems across a possibly dynamic and usually poorly defined set of pathways." The focus of the current study is on the fundamental components of a network which include its *structure* [composed of nodes and links (also called pathways)] and its *dynamics*. The two together specify the network's properties, i.e., its functions and behaviors.

Trust is a multi-dimensional concept and a critical element of modeling any multi-agent behavior in direct or computer-mediated networked interactions. According to ARL, trust management is challenging given that current trust models inadequately capture critical human elements. Modeling such elements such as lack of transitivity, symmetry, and reciprocity requires novel mathematical tools [5]. Any related common quantitative framework would need to include an approach for modeling uncertainty as well as related metrics. Specific to the trust metric is the challenge of understanding its diverse definitions and dimensions to develop a composite trust metric. Modeling of such a metric may need to take into network interactions as well as context- and time-varying nature of its components. The modeling of the composite trust metric discussed later takes into consideration the interactions between the constituent networks, resource constraints and mission goals. The discussion of the composite trust metric is based upon a delineation of the concepts and properties of trust relevant to the constituent elements of a tactical network. The trust metric needs to be derived in a distributed fashion in a mobile and dynamic resource-constrained environment subject to numerous internal and external influences and wherein node captures and subversion can happen. The trust management framework needs to be developed and implemented by further advancing upon the trust metric as well as advancing beyond existing frameworks to match the specific needs of the ad hoc networks.

The outline of the paper is as follows. In section 2 we introduce the wireless mobile *ad hoc* networks characterized by NIST as the next generation wireless communication systems. Section 3 reviews the multidisciplinary foundations of trust and trust management as well as the interrelationship between trust and risk that are central to ARL's ongoing research on such networks. Section 4 presents a survey of the trust management schemes reviewed for defining a trust management model suited to the specific characteristics of mobile ad hoc networks. Section 5 describes a specific case of implementation of the developed trust and trust management models in testing a trust-based task assignment protocol for tactical military networks. Section 6 concludes our discussion outlining directions for future research.

2. Next Generation Wireless Mobile *Ad Hoc* Networks

According to the NIST Advanced Network Technologies Division, next generation wireless communication systems will need to evolve beyond centralized connectivity of today's mobile cellular phone networks. Such *next-gen* (next generation) networks of autonomous mobile self-discovering, self-organizing, and self-adaptive nodes evolving dynamically and unpredictably will be capable of rapid deployment. Going under names such as wireless ad hoc networks, mobile ad hoc networks (MANETs), and wireless sensor networks, they will offer "survivable, efficient and dynamic"[1] (NIST) communications in military battlefield networks (as illustrated in Fig. 1) as well as first responder emergency disaster recovery and rescue operations, heavy construction, mining, transportation, and special event management. The autonomous mobile nodes – hosts also having routing capabilities – will be capable of discovering rapidly and unpredictably changing network topology and delivering messages over relatively bandwidth constrained wireless links. Such mobile nodes will associate extemporaneously on ad hoc basis to form self-forming and self-healing networks and will not rely on centralized resources or fixed infrastructure for peer-level communications. Above distinguishing characteristics of ad hoc networks of highly mobile users or platforms needing to share IP-based information will enable them to deliver secure networking capabilities where "fixed network infrastructure is impractical, impaired, or impossible"[2].

[1] http://www.antd.nist.gov/wahn_mahn.shtml

[2] http://www.cisco.com/c/en/us/products/ios-nx-os-software/mobile-ad-hoc-networking/index.html

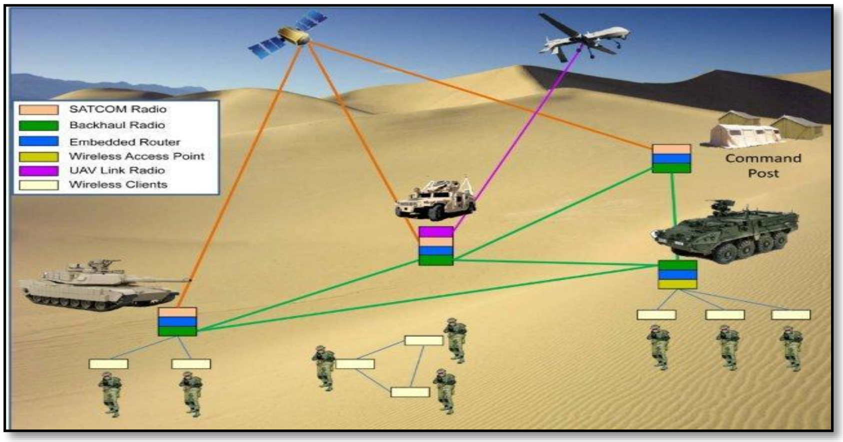

Fig. 1. Radio Aware Routing Protocols Enable Ad Hoc Battlefield Networks
Source: http://eecatalog.com/

The design of network protocols of ad hoc networks is a complex concern given efficient distributed algorithms required for network organization, link scheduling, and routing. The shortest path optimal route algorithms of fixed and centralized wireless paradigm do not generalize to ad hoc networks as network routing should dynamically adapt to various effects. Such effects include variable wireless link quality, propagation path loss, fading, multiuser interference, power usage, and topological changes as well as preservation of security, latency, reliability, prevention of jamming, and recovery from failure in the military battlefield[3]. Particularly, to minimize detection or interception in military contexts, nodes should radiate minimal power and transmit as infrequently as possible lest performance and reliability of the network is degraded or compromised. Section 3 discusses modeling of trust in such networks.

3. Modeling Trust in Mobile Ad Hoc Networks

The self-discovering, self-organizing, and self-adaptive ad hoc network depends on mutual cooperation and trust relationships between autonomous nodes. The nodes depend upon communication of data and control between each other as well as across intermediate nodes. Reliance on intermediate nodes exposes the network to passive and active attacks from malicious nodes. As dependence upon a centralized trust authority is impractical for ad hoc network, cryptographic protocols based on centralized control are not helpful [1]. Hence, trust management is crucial for the nodes in establishing the ad hoc network as well as its execution based on acceptable level of trust especially in absence of any history of prior interactions between those nodes. Computational resource constraints, exposure to eavesdropping, high security threat exposure, inherent vulnerability of wireless, and sudden unpredictable changes in network topology and membership make the above process even more challenging.

[3] http://www.antd.nist.gov/wahn_mahn.shtml

Network security researchers rely upon trust management concepts for developing trust management protocols including trust establishment, trust update, and trust revocation conducive to enabling and sustaining wireless mobile ad hoc networks. Such for ad hoc networks are all the more necessary given uncertainty and incompleteness of continuously changing trust evidence resulting from dynamic nature and characteristics described above.

ARL underscores the overarching focus on managing *uncertainty* and *risk* that encompasses its research on *trust management* in ad hoc wireless networks [5]. Their emphasis is consistent with the observation that the logic of *risk*, including *uncertainty* and *probability*, occupies an important position in defining trust [36]. For developing a common quantitative framework for managing uncertainty, ARL emphasizes metrics development as in the case of trust as a key concern ([5], p. 5): "The scientific challenge is to understand the different definitions and dimensions of trust, for example, in socio-cognitive and communications networks, and from that understanding develop a composite trust metric." The ARL trust management framework builds upon the concept of trust as defined in social sciences as the *degree of subjective belief about the behaviors of a particular entity* [22]. Related focus is on trust management as a unified approach for specifying and interpreting security policies, credentials, and relationships [26].

Defining Trust for Wireless Mobile Ad Hoc Networks

Based on multidisciplinary research survey on trust and trust management [14], ARL developed its communication and networking focused composite metric of trust. This metric was expected to enable trust management of ad hoc networks while accounting for their distinct characteristics and factoring in the relationship between trust and risk. Merriam Webster's Dictionary defines trust as "assured reliance on the character, ability, strength, or truth of someone or something; one in which confidence is placed." In the *Sociological perspective*, *sociological trust* is an assessor's *a priori* subjective probability that a person (or agent, or group) will perform specific actions that affect the assessor [10]. In this view, the notion of trust exists because the trustor is uncertain if the agent (trustee) will perform the action or not in specific circumstances. Thus, in a relationship involving two entities (trustor and trustee) and a specific action, trust is the level of likelihood with which the trustee will perform a specific action before such action can be monitored and in a context in which it affects trustor's own actions [10].

Trust is thus described in terms of *subjectivity*, an indicator for future actions, and *dynamicity* based on continuous interactions between two entities. Applied to computer science, trust is quantified as a continuous variable in the context of acceptance of *risk* while highlighting risking of betrayal as an important aspect of building trust [37]. To be useful, network trust models must capture this subjective aspect of social trust. In the *Economic perspective*, *economic trust* is an expectation that applies to situations in which those who trust take risky actions under uncertainty or incomplete information [16]. The economic perspective also distinguishes between *informal* and *personal trust* between individuals as well as *institutionalized trust* between individuals and institutions such as those involved in extending financial credit to individual entities [35]. Further, while the game theory models [3] emphasize *selfish trust* based on rational strict maximization of individual incentive, altruistic *cooperative trust* [31] can however emerge from initially selfish behaviors. All the above types of trust are relevant to ad hoc networks for instance in the design of selfish nodes and redemption mechanisms. Similar economic models can be used with trust-based encryption primitives for modeling of secure encryption and secure information flows across networks [29].

In the *Philosophical perspective*, trust is *important* as it facilitates benefactor-beneficiary relationships without external [e.g. legal] compliance, but is also *dangerous* given the possibility of betrayal of trust when trustee doesn't behave as expected [8]. The philosophical perspective distinguishes *trust* as a subjective attitude that the trustor has towards trustee (whom she hopes to be trustworthy) from *trustworthiness* which is an objective property, not an attitude. *Trusting thus requires acceptance of risk* of being vulnerable to betrayal [of trust] as there is no clear basis for the motivation of potential trustee as well as the willingness and/or capability of him to do what one trusts him to do [23]. The *Psychological perspective* emphasizes the cognitive process that humans learn trust from their experiences, *psychological trust* being defined as the confidence of finding what is desired from another rather than what is feared [27]. The *Organizational Management perspective* describes *organizational trust* as the extent to which one accepts the risk of being vulnerable to betrayal when one counts on someone or something with a feeling of relative security despite possible negative consequences [11, 13]. The Organizational Management perspective can shed light on how to measure ability, integrity, and benevolence of each node in the ad hoc network as well as how to assess risk in both individual and group modes for self-selected dynamic communities of interest [14].

With increasing complexity of technology given critical need for developing trust in automation, the *Autonomic Computing* perspective focuses on models of how trust in automation is developed and displaced. Given importance of reliance on as well as reliability of technology in case of ad hoc networks, *autonomic trust* is the attitude that an automation or human agent will help accomplish the individual's goal in environment of uncertainty and vulnerability [19]. In the *Communications & Networking perspective*, trust is defined as a set of relations among entities participating in a protocol based on the evidences generated by their prior interactions. Based on prior experience of interactions, trust accumulates based upon the accumulated evidence. Trust is also defined as the degree of belief about the behavior of other agents or entities [24]. *Context-aware trust* is the belief that an entity is capable of performing reliably, dependably, and securely in a *specific context* [15]. Social networks focused on building *social trust* based relationships among entities can be extended to computer science by defining trust as a well-defined descriptor of security and encryption as a metric to reflect security goals

[20]. Above multi-disciplinary nature of trust is depicted in the summary shown in Fig. 2 and underlies ARL's development of the composite trust metric for mobile ad hoc networks.

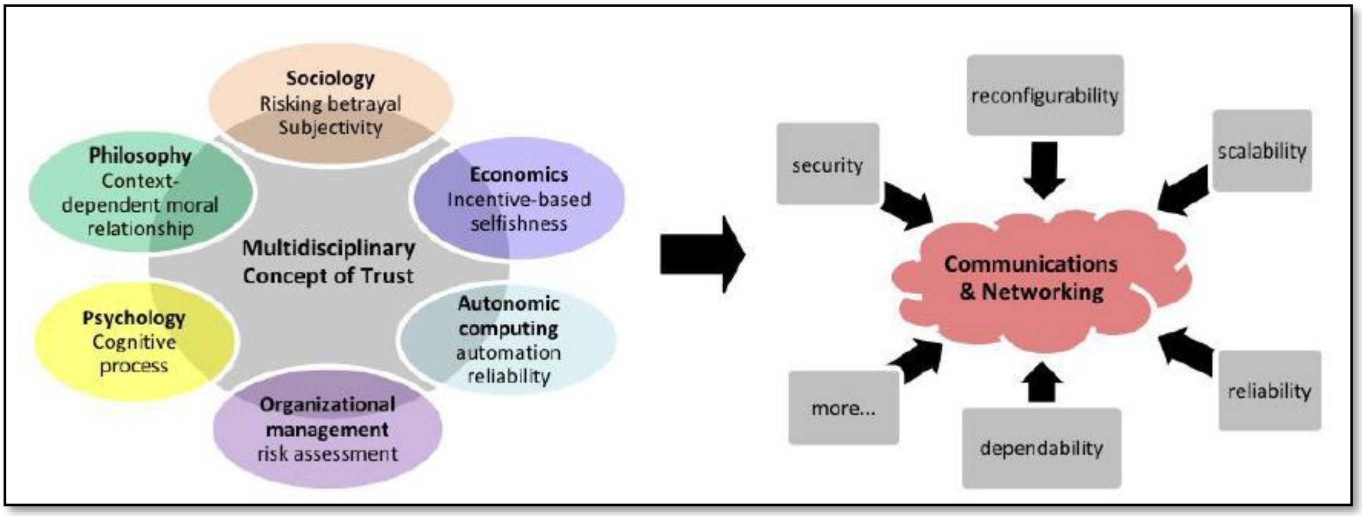

Fig. 2. Multidisciplinary Foundations of Trust and its Network Security Applications
Source: U.S. Army Research Lab

Based upon the above multi-disciplinary review, ARL developed a *trust metric* that had the following characteristics [14]: (1) trust is established based on potential risks, (2) trust is context-dependent, (3) trust is based on selfishness, i.e., on each party's own interests, (4) trust is learned, i.e., it is a cognitive process, (5) trust may represent system reliability.

Distinguishing Trust, Trustworthiness, and Risk

The distinctions and relationships between how trust, trustworthiness, and risk are related are shown in Fig. 3. *Trust* is measured in terms of the *subjective* belief probability of level of trust varying between complete distrust (0) to complete trust (1) on a 0 to 1 scale [4]. In contrast, *trustworthiness* is the *objective* probability that the trustee will behave as expected by the trustor to perform the action on which the interests of the trustor depend [6].

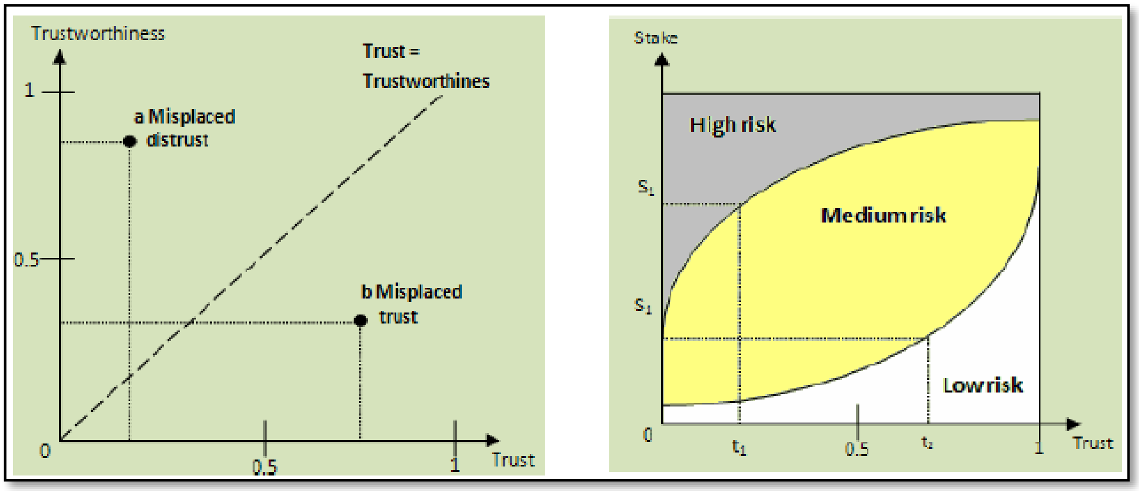

Fig. 3. How Trust, Trustworthiness, and Risk Are Related

Source: U.S. Army Research Lab

The left panel of Fig. 3 [6] shows how the two constructs, trust, i.e., *subjective probability* of trust level, and, trustworthiness, i.e., *objective probability* of trust level are interrelated in influencing the level of risk taken by the trustor in trusting. When both probabilities are equal, it characterizes well-founded trust depicted by the dashed positively sloped line. When the two probabilities are quite different, i.e., further away on either side of the dashed line, inaccurate *risk estimation* and *risk management* on the part of trustor may result. The misplaced trust on the upper side shown by point **a** shows trustworthiness of the trustee far exceeding the trust placed in him or her by the trustor. As a result, because of lack of adequate trust, the trustor may forego many beneficial opportunities of cooperating given relative high trustworthiness of the trustee. On the other hand, the misplaced trust on the lower side shown by point **b** denotes trust placed by the trustor in the trustee far exceeding the trustee's trustworthiness. As a result, because of too much trust, the trustor may end up trusting the trustee even when such trust is not warranted, i.e., high risk of betrayal in terms of the trustee not actually doing what the trustor expected him or her to do in trustor's interests.

The right panel of Fig. 3 shows the variation in risk as a function of the stake (y-axis) and the risk (x-axis). Regardless of the estimated true value, when the stake is too high, the value of risk is considered as high and when the stake is too low the value of risk is considered too low. Typically, risk is low when trust value is high, however as seen in Fig. 3, at higher stake such as with increased risk probability, risk is higher even when the level of trust is hundred percent at 1.0. Given such risk-return trade-offs related to various values on the continuum of trust, trust is generally neither proportional nor inversely proportional to risk [6]. Hence, careful risk estimation is associated with modeling accurate trust relations between the nodes in the network. Such trust relations may also be distinguished in terms of *reliability trust* which is non-specific to any context and *decision trust* which is specific to decision specific to a given context or outcome expected by the trustor.

Trust Properties in Wireless Mobile Ad Hoc Networks

Given their unique properties and inherent unreliability of the wireless channel, trust in mobile ad hoc networks is dynamic, subjective, not necessarily transitive, asymmetric, and context-sensitive [14]. Each of these characteristics of trust in ad hoc networks is illustrated in Fig. 4 and discussed further.

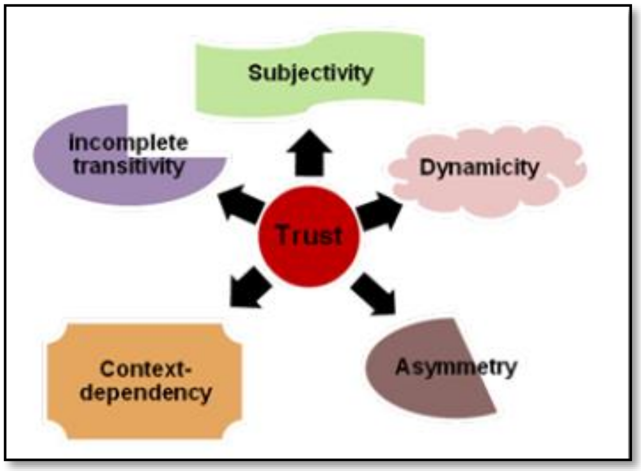

Fig. 4. Trust Properties in Wireless Mobile Ad Hoc Networks
Source: U.S. Army Research Lab

Trust establishment in ad hoc networks should be *dynamic* and not static [33] being dependent on incomplete and rapidly changing temporal and spatial information because of node mobility and/or failure. Given dynamically changing network topology, each node will need to reassess and adjust its trust continuously given cumulative experience history with respect to other nodes, hence trust is *subjective*. Trust is *not necessarily transitive* [38] in the sense that Alice may trust Bob and Bob may trust Charles, but Alice may not trust Charles. Trust is *asymmetric* as the nodes with higher capabilities may not trust other nodes with lesser capabilities at the same level that nodes with lesser capabilities trust them [2]. Such asymmetry of trust may also relate to the level and scope of benefits that the nodes with higher capabilities are able to provide for nodes with lesser capabilities and vice-versa. Trust is context-sensitive as the trustor node may trust the trustee node for some specific actions and not for others. Next section builds upon the above discussion to develop the trust management model for mobile ad hoc networks.

4. Modeling Trust Management in Mobile Ad Hoc Networks

Trust management needs to be distinguished from *reputation management* given both are relevant to modeling trust [15]. While *trust* is the subjective belief of a node about trust level in its peer, *reputation* is the perception that peers form about a node. *Recommendation* is the mechanism for communicating reputation of a node from one community context to another. Similarly, *trust management* and *trust establishment* need to be distinguished [12]. Trust management deals with formulating evaluation rules and policies, representation of trust evidence, and evaluation and management of trust relationships whereas trust establishment deals with representation, evaluation, maintenance and distribution of trust among nodes. Trust management thus includes trust establishment, trust update, and trust revocation as illustrated in Fig. 5. Trust management can also be considered as a special case of risk management with focus on authentication of entities under uncertainty and decision-making on cooperation with unknown entities.

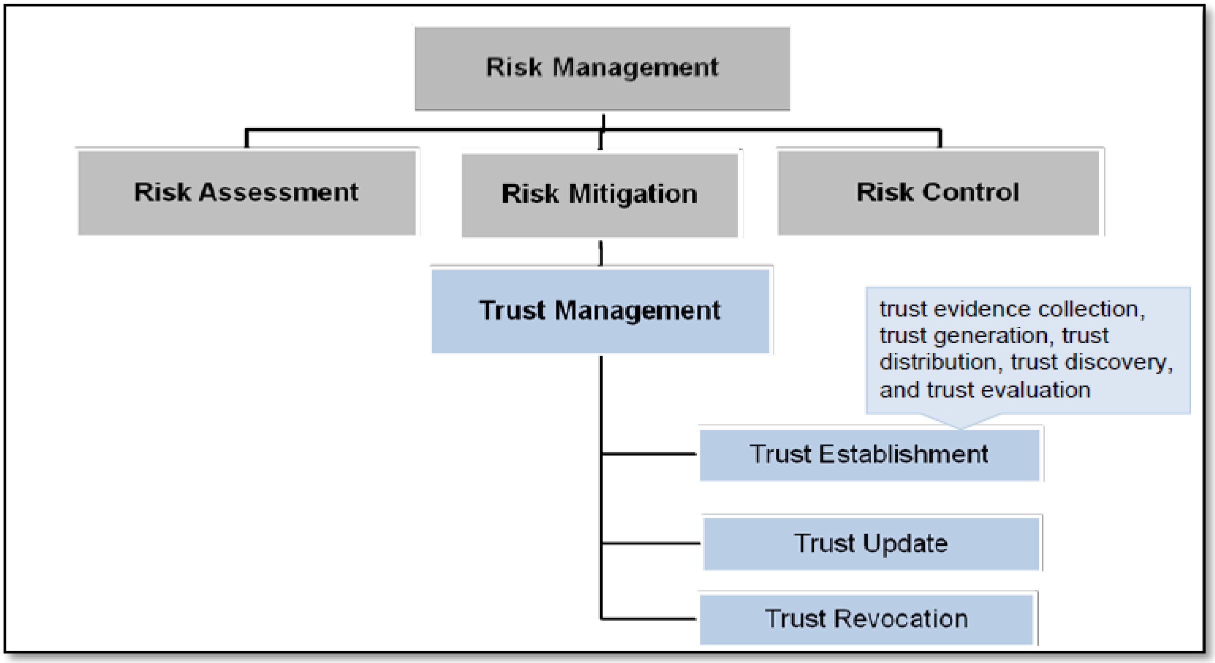

Fig. 5. Risk Management, Trust Management, and Related Activities
Source: U.S. Army Research Lab

Trust Management Modeling Classifications

In the context of mobile ad hoc networks, the scope of trust management is expanded to go beyond authentication to also include secure routing, intrusion detection, key management, access control, and other control mechanisms. Trust management may be classified into two frameworks: *trust establishment framework* and *reputation-based framework* [32, 21]. In the trust establishment framework, trust is established between adjacent nodes based upon direct interactions, and, between non-adjacent nodes based on aggregated opinions of intermediate nodes. In reputation based framework, direct interactions with a node as well as indirect recommendations about it from other nodes is used for evaluating its trust. Evaluation of trust can be further done using *policy-based trust management* or *reputation-based trust management*.

Policy-based trust management makes binary decisions about the trustworthiness of the node based upon objective security schemes such as verifiable properties in signed credentials for access control. Reputation-based trust management is more flexible as it uses numerical and computational mechanisms that compute trust as a continuous variable by aggregating reputation from across the various nodes.

Trust management may also be distinguished in terms of *evidence-based trust management* and *monitoring-based trust management* [15]. Evidence-based trust management relies upon challenge and response based evidence produced by any node for itself or for other nodes or artefacts such as public key, address, or identity that proves trust relationships between nodes. In contrast, monitoring-based trust management depends upon direct and indirect observations about nodes where direct observations focus on malicious and/or selfish behaviors of adjacent nodes and indirect observations rely on reputation ratings such as recommendations of other nodes. Trust establishment frameworks can be distinguished into *certificate-based frameworks* and *behavior-based frameworks* [12]. The certificate-based frameworks make use of trust decisions based on a valid certificate issued by other trustworthy nodes as a proxy of the trustworthiness of the respective node. Behavior-based frameworks use preloaded authentication mechanisms and base their trust evaluations upon monitoring of the behavior of the adjacent nodes. Trust establishment schemes can also be classified according to the architectures used as *hierarchical framework* and *distributed framework* [12]. Hierarchical framework relies upon centralized certificate authorities or trusted third parties for trust evidence for hierarchy of nodes based on capabilities or levels of trust. In contrast, distributed framework, as in the case of wireless mobile ad hoc networks, relies upon each node with often equal capability to acquire, maintain, and distribute trust evidence in absence of a centralized infrastructure.

Network Security Attacks Relevant to Trust Management

Potential attacks that can subvert or compromise the trust management system need to be taken into consideration in trust management modeling. Surveys of threat models and attacks relevant to the wireless mobile ad hoc network routing protocols are available in prior research [30, 9]. Attacks can be distinguished as *passive attacks* vs. *active attacks* [39] and *insider attacks* vs. *outsider attacks* [7]. Attacks wherein adversary gains access to an asset but doesn't modify its contents are called passive attacks: examples of which include eavesdropping and traffic analysis. Active attacks that modify a message, data stream, or file include one or more of the combinations of the following attacks: masquerade, replay, message modification, and denial-of-service. Insider attacks are attacks caused by authorized or privileged users who use the system in unauthorized or malicious manner such as by exploiting poor configurations or bugs in privileged programs. Outsider attacks are caused by unauthorized or non-privileged users typically by gaining access to an authorized or privileged account. Trust management schemes are designed to detect both selfish and malicious nodes so that the trust evaluation engine degrades gracefully if some evidence is corrupted because of the attacks. In addition to the above surveys of trust management, a survey of attacks that include routing loop attacks, wormhole attacks, blackhole attacks, grayhole attacks, DoS attacks, false recommendation attacks, incomplete information attacks, packet modification attacks, newcomer attacks, Sybil attacks, blackmailing attacks, replay attacks, etc. is available in Cho et al. [14].

Metrics for Ad Hoc Network Trust and Trust Management Modeling

Based on a research survey of trust management schemes and evaluation of trust for wireless mobile ad hoc networks, Cho et al. [14] observe that prior research doesn't clearly address what should be *measured* to evaluate network trust. Following on that observation, they propose two types of trust representing different aspects of network trust for ad hoc networks: *Social Trust* and *Quality of Service (QoS) Trust*. Extending research on social relationships in social networks of loose relationships with common interests [17], social trust characterizes the properties based upon such social relationships. Examples of social trust based on social relationships include friendship, honesty, privacy, and social reputation/recommendation based upon direct or indirect "sociable" interactions. The analogs of social trust in case of mobile wireless ad hoc networks include frequency of communications of nodes, malicious or benign behaviors of nodes (e.g., false accusation, impersonation), and quality of reputation of nodes. In contrast to the "sociable" interactions focused social trust, QoS trust has its primary focus of trust evaluation in terms of task performance capability. Examples of QoS trust from social networks extended to mobile ad hoc networks include competence, dependability, reliability, successful experience, and reputation/recommendation on task performance based upon direct and indirect interactions. Other specific examples of QoS trust specific to ad hoc network protocols include performance metrics of trust value such as a node's energy or computational power, lifetime, packet delivery rate, and, task performance evaluations using reputation or recommendation.

Standard system performance metrics used for evaluating trust management systems include trust level, route usage (for secure routing), throughput, goodput, overhead, delay, utility, packet dropping rate, detection accuracy, etc. While detection accuracy is a common trust management performance metrics, trust metrics such as trust value, trustworthiness, and, trust level per session are also used commonly for evaluating trust management schemes [14].

Various trust management schemes have been developed for mobile ad hoc networks. Such schemes can be described based on specific design purposes such as secure routing, authentication, key management, intrusion detection, access control, and other control mechanisms. *Secure Routing* deals with isolation of misbehaving nodes, either selfish or malicious while encouraging collaboration. It also includes reputation-based trust management, extension of the existing routing protocols (e.g., DSR, AODV) using trust concept, incentive and redemption mechanisms. Secure routing related trust models include Bayesian model, entropy-based model, probability model, and effort-return-based model.

Authentication based trust management schemes may be direct (based on certificate, or direct observations) plus second hand information (e.g., recommendation), or, extensions of the existing routing protocols (e.g., DSR, ZRP), and use weighted transitivity. Authentication related trust models include Marsh's trust model [34] and PGP. *Key Management* based trust management schemes are based upon trust-based hierarchies for key management, physical logical trust domains, and, hierarchical trust PKI and use distributed key management models. *Intrusion Detection* based trust management schemes use an IDS to provide audit and monitoring capabilities that offer the local security to a node and help perceive the specific trust level of other nodes. Evaluating trust and identifying intrusions may however not be a separable process with same goal of building collaborative network environments. *Access Control* based trust management schemes determine access to certain resources or rights in mobile ad hoc networks and use trust-based admission control that consists of a localized group trust model based on threshold cryptography. Others trust management schemes include trust evaluation; trust evidence distribution based upon directed graph or swarm intelligence, and, trust computation based on random graph theory. Based upon the above discussion on the trust model and trust management model, the next section implements these models for testing the composite trust based task assignment protocol.

5. Testing the Composite Trust Based Task Assignment Protocol

Based on prior discussion, we established that trust is the degree of a subjective belief about the behaviors of a particular entity and denotes trustor's willingness to take a risk. Characteristics of trust included its use as a measure of potential risks, context-dependency, subjectivity, system reliability, and based upon cognitive learning process. We also determined that trust management is a separate component of security services in networks. In this section, the above models of trust and trust management are applied to test a trust based task assignment protocol for a tactical military network [28]. Recent and ongoing research conducted by ARL on modeling trust and trust management for wireless mobile ad hoc networks attempts to address the following limitations in prior research [28]. It goes beyond assigning a single node by assigning multiple tasks to an entity and multiple entities to one task. It reflects the context-dependent characteristic of trust in its modeling of the critical tradeoff between trust and risk in the context of task assignment (and associated risk management). It specifically accounts for the required trust level for each task by using a composite trust metric for modeling the missions in terms of the task characteristics.

The task assignment focus is on efficient and effective task assignment in tactical military networks which is key to successful mission completion where the best match between entities and tasks can maximize mission completion ratio. The specific modeling focuses on four types of nodes of node types NT_n where $n = 1, 2, 3, 4$ shown in Fig. 6 with higher value of i denoting higher and more versatile capabilities. NT_n for $n = 1, 2$ have capabilities such as QoS that both humans and machines have in common. NT_n for $n = 3, 4$ have capabilities such as Social Trust that only humans possess. Note that Social Trust and QoS were earlier discussed as the two aspects of the composite trust metric used for modeling of trust and trust management. It is hypothesized that the trust-based soft security approach can increase mission completion ratio in presence of untrustworthy entities where traditional security services may not be practical [28].

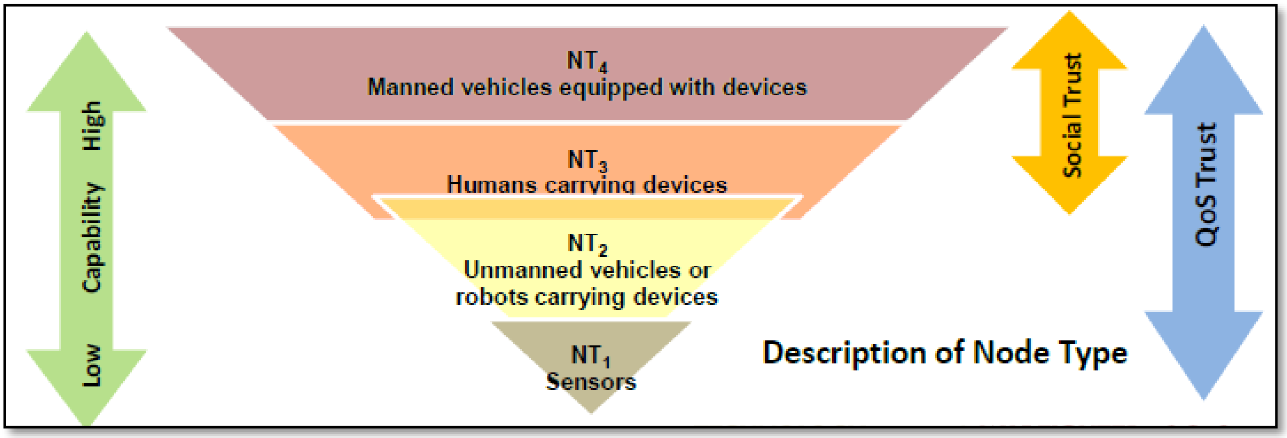

Fig. 6. Node Types and Associated Capabilities and Trust Metrics
Source: U.S. Army Research Lab

Further to prior discussion on the trust metrics Social Trust and QoS, each of the two have the following Trust Properties with associated meanings. *Social Trust* is composed of two Trust Properties: (i) *Social Connectedness*: representing the number of connections in a node's social network, and, (ii) *Reciprocity*: representing the degree of mutual receiving and giving, i.e., when a favor is received an entity tends to return something for the past favor. Similarly, *QoS Trust* is composed of two Trust Properties: (i) *Competence*: representing an entity's capability to service the received request, and, (ii) *Integrity*: Honesty of an entity in attack behaviors. Each task has unique and common task properties. *Unique Task Properties* include the minimum required node type NT$_n$, and, minimum trust threshold for each trust property X (X∈T, where T is the set of trust properties) of task m denoted as T_m^{X-th}. *Common Task Properties* include Importance, Urgency, and Difficulty each defined on an integer scale of 1-5 (from low to high) as follows:

I_m is the Importance of task m in terms of impact expected upon mission completion after the given task failure,

U_m is the Urgency of task m in terms of how urgently the specific task should be completed,

D_m is the Difficulty of task m in terms of how much workload is required to execute the given task.

The specified goal is the development of a trust-based task assignment protocol which maximizes mission completion (ratio) probability $P_m^{completion}$ while meeting an acceptable risk level P_m^{risk} using the composite trust metric [28]. Specified quantitatively, the objective function of a task leader (TL) for task *m* is specified as:

$$\text{Maximize } P_m^{completion}(\text{t}), \text{ given } \sum_{j \in M} r_{m,j}\,(t) \leq P_m^{risk}$$

Where,

$P_m^{completion}$(t) is the completion probability of task *m* at time *t*,

P_m^{risk} is the acceptable risk threshold for task *m*, which can be binary (0 or 1) contingent on task completion at time *t* and is given by:

$$P_m^{risk} = e^{-\rho_2 I_m}$$

Where I_m is the task importance of task m and ρ_2 is a constant normalization parameter,

M is the set of task members (nodes) *j* assigned to task *m*,

$r_{m,j}$(t) is the average risk probability among all trust properties X and is given by:

$$r_{m,j}(\mathrm{t}) = \frac{\sum_{X \in T} r_{m,j}^{X}\,(t)}{|T|}$$

Where,

T is the set of trust properties *X*,

$r_{m,j}^{X}\,(t)$ is the risk probability when node *j* is selected to execute task *m* or is currently executing task *m* at time *t* and is given by:

$$r_{m,j}^{X}\,(t) = e^{-\rho_1 \frac{T_{i(m),j}^{X}(\mathrm{t})}{T_m^{X-th}}\,\frac{U_m}{U_m^{max}}\,\frac{D_m}{D_m^{max}}}$$

Where,

T_m^{X-th} is the minimum trust threshold for a node to execute task *m* without increasing the risk level above task *m*'s acceptable risk threshold P_m^{risk} discussed above,

$T_{i(m),j}^{X}$ is node j's trust evaulated by TL *i*(*m*) (node *i* as task leader for task *m*),

ρ_1 is the constant parameter determined based on the acceptable risk threshold P_m^{risk} to ensure that the acceptable risk level is below it if $T_{i(m),j}^{X} \geq T_m^{X-th}$,

U_m is the urgency value of task *m* specified on integer scale 1-5 with 5 being highest urgency,

D_m is the difficulty value of task *m* specified on integer scale 1-5 with 5 being highest difficulty,

U_m^{max} is maximum task urgency and D_m^{max} is maximum task difficulty among all tasks.

P2P trust evaluation by each node toward other nodes, "subjective trust," is denoted as trust value $T_{i,j}^{X}$ (t) that trustor node *i* evaluates towards trustee node *j* in trust property *X* at time *t*. $T_{i,j}^{X}$ (t)∈R in range [0, 1] where 1 = complete trust, 0.5 = ignorance, and 0 = distrust is based upon both *direct trust* evidence $T_{i,j}^{D-X}$and *indirect trust* evidence $T_{i,j}^{ID-X}$and computed as follows:

$$T_{i,j}^{X}(\mathrm{t}) = \alpha T_{i,j}^{D-X}(\mathrm{t}) + (1-\alpha) T_{i,j}^{ID-X}(\mathrm{t}) \qquad \text{where } 0 < \propto < 1.$$

The parameter α denotes relative weight of direct and indirect trust evidences with larger α implying greater weight of direct trust evidence [18]. The *direct trust* evidence $T_{i,j}^{D-X}$and *indirect trust* evidence $T_{i,j}^{ID-X}$are shown in Fig. 7 and further explained below.

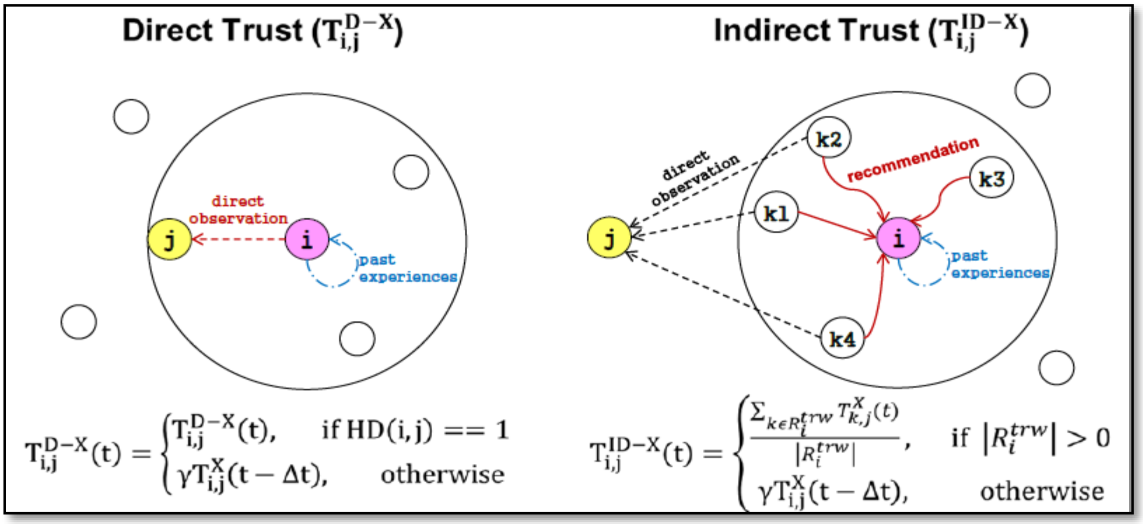
Direct Trust ($T_{i,j}^{D-X}$)
Indirect Trust ($T_{i,j}^{ID-X}$)
direct observation
j
i
past experiences
direct observation
recommendation
k1
k2
k3
k4
j
i
past experiences
$T_{i,j}^{D-X}(t) = \begin{cases} T_{i,j}^{D-X}(t), & \text{if } HD(i,j) == 1 \\ \gamma T_{i,j}^{X}(t-\Delta t), & \text{otherwise} \end{cases}$
$T_{i,j}^{ID-X}(t) = \begin{cases} \frac{\sum_{k \epsilon R_i^{trw}} T_{k,j}^{X}(t)}{|R_i^{trw}|}, & \text{if } |R_i^{trw}| > 0 \\ \gamma T_{i,j}^{X}(t-\Delta t), & \text{otherwise} \end{cases}$

Fig. 7. Modeling Trust Metrics of Direct Trust & Indirect Trust
Source: U.S. Army Research Lab

Direct trust of node i in node j, $T_{i,j}^{D-X}(\mathrm{t})$, represents trust evaluation based on node i's direct observation or experience of node j and is updated as follows.

$$T_{i,j}^{D-X}(\mathrm{t}) = \begin{cases} T_{i,j}^{D-X}(\mathrm{t}) & if\ HD(i,j) == 1 \\ \gamma T_{i,j}^{X}(\mathrm{t}\ - \Delta\mathrm{t}) & otherwise \end{cases}$$

Where,

$HD(i,j)$ is the hop distance or the number of hops between i and j,
Δt is the periodic trust update interval,
γ is decay factor to account for the trust decay over time without further interactions.

Indirect trust of node i in node j, $T_{i,j}^{ID-X}(\mathrm{t})$, represents trust evaluation based on node i's indirect evidence of node j such as recommendations about node j from third parties such as node i's 1-hop neighbors and is updated as follows.

$$T_{i,j}^{ID-X}(\mathrm{t}) = \begin{cases} \dfrac{\sum_{k \in R_i^{trw}} T_{k,j}^{X}\ (t)}{|R_i^{trw}|} & if\ |R_i^{trw}| > 1 \\ \gamma T_{i,j}^{X}(\mathrm{t}\ - \Delta\mathrm{t}) & otherwise \end{cases}$$

Where $R_i^{trw}$is set of 1-hop neighbors of node i providing recommendations towards node j.

Trust-based risk analysis underlies the trust management model of task assignment and task allocation to specific nodes that bid for a specific task [18]. The TL decides between multiple bids received from multiple nodes so that they meet a certain level of trust per property X required by the task while not causing the task to fall below an acceptable risk level. As discussed earlier, the objective function of a task leader (TL) for the specific task *m* is specified as:

$$\text{Maximize } P_m^{completion}(\text{t}), \text{ given } \sum_{j \in M} r_{m,j}\,(t) \leq P_m^{risk} \quad \text{s.t.}$$

average risk probability among all trust properties X: $r_{m,j}(\text{t}) = \dfrac{\sum_{X \in T} r_{m,j}^{X}\,(t)}{|T|}$ and

risk probability when node *j* is selected to execute task *m* or is currently executing task *m*:

$$r_{m,j}^{X}\,(t) = e^{-\rho_1 \frac{T_{i(m),j}^{X}(\text{t})}{T_m^{X-th}}}\, \frac{U_m}{U_m^{max}}\, \frac{D_m}{D_m^{max}}\,.$$

As shown in Fig. 8, trust-based risk analysis is considered in conjunction with the net gain by performing the specific task m for the specific node that bid on the task fitting its schedule availability and capability (denoted by node type NT*n*).

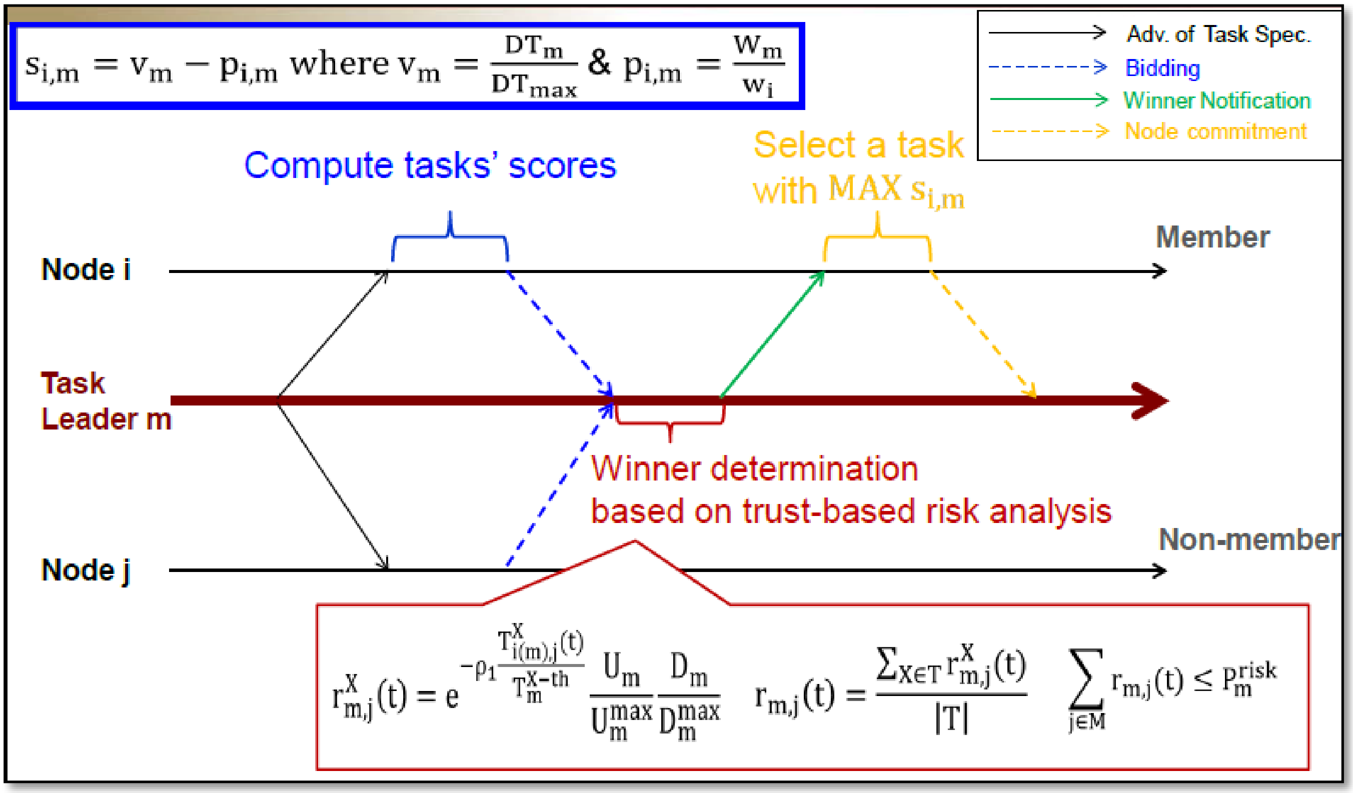
$s_{i,m} = v_m - p_{i,m}$ where $v_m = \frac{DT_m}{DT_{max}}$ & $p_{i,m} = \frac{W_m}{w_i}$
Adv. of Task Spec.
Bidding
Winner Notification
Node commitment
Compute tasks' scores
Select a task with MAX $s_{i,m}$
Member
Node i
Task Leader m
Winner determination based on trust-based risk analysis
Non-member
Node j
$r_{m,j}^{X}(t) = e^{-\rho_1 \frac{T_{i(m),j}^{X}(t)}{T_m^{X-th}}} \frac{U_m}{U_m^{max}} \frac{D_m}{D_m^{max}}$
$r_{m,j}(t) = \frac{\sum_{X \in T} r_{m,j}^{X}(t)}{|T|}$
$\sum_{j \in M} r_{m,j}(t) \leq P_m^{risk}$

Fig. 8. Testing the Composite Trust Based Task Assignment Protocol

Source: U.S. Army Research Lab

The bidding node's net gain or 'score' is computed as follows:

$$s_{i,m} = v_{i,m} - p_{i,m} \quad \text{where}$$

$s_{i,m}$ is the net gain or score of node i for performance of task m,

$v_m = \frac{DT_m}{DT_{max}}$ is valuation of performance of task m based on the relative length of task duration, i.e., ratio of duration for task m (DT_m) to maximum duration among all tasks (DT_{max}) based on the premise of greater access to resources and higher trust level by continuous interactions,

$p_{i,m} = \frac{W_m}{w_i}$ is the 'price' or 'cost' incurred by node i to perform task m, the ratio of the required workload per time unit by task m (W_m) to node i's maximum capability to handle workload per time unit (w_i).

The above case study focused on the modeling of trust and trust management for designing security protocols for mission-driven group communication wireless mobile ad hoc networks. The specific focus of trust and trust management modeling was on the evaluation of trust level of such a network by evaluating the trust value of a node in terms of its mission execution competence and sociability when a particular mission, M, is assigned. For example, each node is evaluated by asking "Can we trust this node to do mission M?" [18] As a result, the trust management protocol dynamically reconfigures the trust threshold to determine the nodes qualified for performing the mission. The detailed trust management protocol factors in the level of risk or difficulty while considering changing network conditions as well as the conditions of participating nodes. The resulting trust protocols seek to prolong system lifetime by optimizing mission performance factors such as trust value threshold to determine trustable nodes, trust transitivity chains, ratios of trust types, threshold of selfish behaviors, and length of trust chains for optimally balancing security and performance properties.

6. Conclusion

Given critical role of both Trust and Trust Management in Network Security protocols, it is critical to understand how they are being modeled and applied in most advanced high security networking environments. Such understanding can serve as a foundation for modeling, design, and implementation of next generation mobile wireless networks for other high security environments such as in Banking & Finance. The current study focused on understanding the modeling and implementation of Trust and Trust Management for next generation wireless communications systems, specifically mobile ad hoc networks, by the ARL

Computational and Information Sciences Directorate. Specifically, we examined the capabilities afforded by the next generation wireless mobile ad hoc networks, how trust and trust management are modeled in such mobile ad hoc networks; and, how trust and trust management are implemented in trust-based task assignment in tactical networks.

The specific choice of the military mobile ad hoc networks as focus of the case study was motivated by the most adverse hostile and challenging cyber security environments in which such networks need to survive. Factors that challenge mission critical survival and competence of such high security mobile ad hoc networks include ability to participate in coalition operations without predefined trust relationships, supporting prioritized QoS performance, dealing with compromised nodes, resource constraints, vulnerability, unreliable transmission medium, and dynamics. The specific choice of the ARL Network Science research program was also motivated by its leading-edge focus on the mathematical modeling of social networks based next-generation mobile wireless networks trust management protocols. Given their integrated dualistic focus on both social networks based *social trust* modeling *and* the capability of executing high risk mission based on *QoS trust* modeling, they offer a very interesting prototype for other high security application areas. Specific high security application areas that come to mind include Global Banking and Finance applications in which social networks and social media are playing an increasingly critical role. Future research plans to further understand how such trust and trust management models and protocols can be applied in those real world contexts.

Bibliography

[1] A. A. Pirzada, C. McDonald, "Establishing trust in pure ad-hoc networks," in: CRPIT '04: Proceedings of the 27th Conference on Australasian Computer Science, Australian Computer Society Inc., Darlinghurst, Australia, 2004, pp. 47–54.

[2] A. Abdul-Rahman and S. Hailes, "Using Recommendations for Managing Trust in Distributed Systems," Proc. IEEE Malaysia Int'l Conf. on Communication, Kuala Lumpur, Malaysia, Aug. 1997.

[3] A. B. MacKenzie and S. B. Wicker, "Game Theory and the Design of Self-Configuring, Adaptive Wireless Networks," IEEE Commun. Mag., vol. 39, no. 11, pp. 126-131, Nov. 2001.

[4] A. Josang and S. LoPresti, "Analyzing the Relationship between Risk and Trust," Proc. 2nd Int'l Conf. Trust Management, LNCS, Springer- Verlag, 2004, pp. 135-145.

[5] A. Swami and B. J. West, Editors, Research@ARL Network Sciences, 2013.

[6] B. Solhaug, D. Elgesem, and K. Stolen, "Why Trust is not proportional to Risk?" Proc. 2nd Int'l Conf. on Availability, Reliability, and Security, 10-13 Apr. 2007, Vienna, Austria, pp. 11-18.

[7] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless Network Security-Signals and Communication Technology, Part II, 2007, pp. 103-135, Springer U.S.

[8] C. McLeod, "Trust", The Stanford Encyclopedia of Philosophy (Summer 2014 Edition), Edward N. Zalta (ed.), URL = <http://plato.stanford.edu/archives/sum2014/entries/trust/>.

[9] D. Djenouri, L. Khelladi and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," IEEE Commun. Surveys and Tutorials, vol. 7, no. 4, pp. 2-28, 2005.

[10] D. Gambetta, "Can We Trust Trust?" Trust: Making and Breaking Cooperative Relations, Basil Blackwell, Oxford, 1990, pp. 213-237.

[11] D. McKnight and N. Chevany, "The Meanings of Trust," Carlson School of Management, University of Minnesota, Technical Report TR 94-04, 1996.

[12] E. Aivaloglou, S. Gritxalis, and C. Skianis, "Trust Establishment in Ad Hoc and Sensor Networks," Proc. 1st Int'l Workshop on Critical Information Infrastructure Security, Lecture

Notes in Computer Science,vol. 4347, pp. 179-192, Samos, Greece, 31 Aug. – 1 Sep. 2006, Springer.

[13] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "An Integrative Model of Organizational Trust: Past, Present, and Future," Academy of Management Review, vol. 31, no. 2, 2007, pp. 344-354.

[14] H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Communications Surveys Tutorials, vol. 13, no. 4, pp. 562–583, 2011.

[15] H. Li and M. Singhal, "Trust Management in Distributed Systems," Computers, vol. 40, no.2, Feb. 2007, pp. 45-53.

[16] H. S. James, "The Trust Paradox: A Survey of Economic Inquiries into the Nature of Trust and Trustworthiness," Journal of Economic Behavior and Organization, vol. 47, no. 3, 2002.

[17] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," IEEE/ACM Transactions on Networking, vol. 16, no. 3, June 2008, pp. 576-589.

[18] I. R. Chen, F. Bao, M. Chang, J. H. Cho, "Integrated Social and QoS Trust-based Routing in Delay Tolerant Networks," Wireless Personal Communications, pp. 1-17, June 2011.

[19] J. D. Lee and K. A. See, "Trust in Automation: Designing for Appropriate Reliance," Human Factors, vol. 46, no. 1, Spring 2004, pp. 50-80.

[20] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks, Baltimore, MD, 28 Aug. – 1 Sep. 2006, pp. 1-7.

[21] J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks," IEEE Commun. Mag., vol. 46, no. 4, Apr. 2008, pp. 108-114.

[22] K. S. Cook (editor), Trust in Society, vol. 2, Feb. 2003, Russell Sage Foundation Series on Trust, New York.

[23] K. Jones, "Trust as an Affective Attitude," Ethics, 107: 4–25,1996.

[24] L. Capra, "Toward a Human Trust Model for Mobile Ad-hoc Networks," Proc. 2nd UK-UbiNet Workshop, 5-7 May 2004, Cambridge University, Cambridge, UK.

[25] L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.

[26] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management." Proceedings of IEEE symposium on security and privacy; 1996. pp. 164–73.

[27] M. Deutsch, The Resolution of Conflict: Constructive and Destructive Processes, Carl Hovland Memorial Lectures Series, New Haven and London: Yale University Press, 1973.

[28] M. J. Chang, J.H. Cho, I.R. Chen, K.S. Chan, and A. Swami, "Trust-based Task Assignment in Military Tactical Networks," 17th Int'l Command and Control Research and Technology Symposium, Fairfax, VA. 19-21 June, 2012.

[29] M. Srivatsa, S. Balfe, K. G. Paterson, and P. Rohatgi, "Trust Management for Secure Information Flows," Proc. 15th ACM Conf. on Computer and Communications Security, Alexandria, VA, Oct. 2008, pp. 175-188.

[30] P. G. Argyroudis and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks," IEEE Commun. Surveys and Tutorials, vol. 7, no. 3, pp. 2-21, 2005.

[31] R. Axelrod, "The Evolution of Cooperation," Science, vol. 211, no. 4489, pp. 1390-1396, March 1981.

[32] R. Li, J. Li, P. Liu, H. H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," Proc. IEEE 65th Vehicular Technology Conf., 22-25, Apr. 2007, pp. 56-60.

[33] R. Parasuraman, "Humans and Automation: Use, Misuse, Disuse, Abuse," Human Factors, vol. 39, no. 2, 1997, pp. 230-253.

[34] S. Marsh, "Formalizing Trust as a Computational Concept," Ph. D. Dissertation, Department of Mathematics and Computer Science: University of Stirling, 1994.

[35] T. Harford, "The Economics of Trust," Forbes, Nov. 3, 2006. http://www.forbes.com/2006/09/22/trust-economy-markets-tech_cx_th_06trust_0925harford.html

[36] T. K. Das and B.S. Teng (2004). "The Risk-based View of Trust: A Conceptual Framework," Journal of Business and Psychology, 19 (1) 85–116.

[37] W. J. Adams, N. J. Davis, "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration," Proc. 6th Annual IEEE SMC Information Assurance Workshop, 15-17 June, 2005, West Point, NY, pp. 317-324.

[38] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, Feb. 2006, pp. 305-317.

[39] Z. Liu, A. W. Joy, and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," Proc. 10th IEEE Int'l Workshop on Future Trends of Distributed Computing Systems, Sushou, China, 26-28 May 2004, pp. 80-85.