2014 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
AUTONOMOUS GROUND SYSTEMS (AGS) TECHNICAL SESSION
AUGUST 12-14, 2014 – NOVI, MICHIGAN

SOFT SECURITY CONSIDERATIONS FOR UNMANNED SYSTEMS

Dariusz Mikulski, Ph.D.
Ground Vehicle Robotics
U.S. Army TARDEC
Warren, MI

ABSTRACT

This paper discusses various soft security considerations that should be accounted for in the next generation of advanced military unmanned systems. By modeling unmanned system teams as mobile ad hoc networks, we underscore the different types of information-based security vulnerabilities that motivated adversaries may be able to exploit in unmanned systems. Then we provide an overview of computational trust and show that it can be used to defend against these vulnerabilities by finding the most reliable agents to interact with from a pool of potential agents. Finally, we discuss ongoing work at U.S. Army TARDEC that is applying computational trust within a vehicle controller for autonomous convoy operations.

INTRODUCTION

As doctrine, the Pentagon has formally recognized cyberspace as a new domain in warfare, which has become just as critical to military operations as land, sea, air, and space [1]. And evidence in recent media reports indicates that other nation-states are actively developing their own cyber attack capabilities to break into or disrupt unmanned systems [2] [3] [4] [5]. We can expect that these cyber attack capabilities will only become more sophisticated in time. We can also extrapolate that as more unmanned systems are introduced into military operations, the value of attacking these assets will be higher. As such, it is certain that our nation will be more exposed to these types of attacks and vulnerabilities in the future, which puts American warfighters and U.S national security interests in jeopardy.

Prior to 2003, the U.S. military had no fielded unmanned ground vehicles [6], despite Congress's goal in 2001 that "by 2015, one-third of operational ground combat vehicles are unmanned [7]." But over the past decade, more than 12,000 unmanned ground vehicles have been fielded for use in Iraq and Afghanistan [6]. These first-generation systems were largely tele-operated by a single warfighter and tailored to a narrow mission [8], but their usefulness has spurred demand for more robotic capabilities across a broader spectrum of military operations [9] [10]. This signals that a growth in cooperative teaming capabilities is necessary to meet the needs for the next generation of military robots.

Often, it is convenient to assume that unmanned systems within the same team should be regarded as fully trustworthy for cooperative tasks because of the complexity involved in producing robust, autonomous multi-robot solutions. However, military unmanned systems, with their unique exposure to cyber attacks, are at increased risk for mission failure which can also endanger the lives of friendly forces. Hard security mechanisms, such as cryptography protection and authentication protocols, are vital to minimizing this exposure. However, hard security mechanisms cannot protect against illegitimate behaviors after a hard security event, such as decryption or identification validation. Hencethe need for soft security – a requirement to defend against the threat of unwanted or undesired behavioral changes in a system [11] . This is an additional security layer in which each unmanned system monitors the behaviors of others to ensure that everyone else is behaving appropriately. Computational trust models, which dynamically adjust to observed behaviors or recommendations, are excellent tools that improve soft security and mitigate the risks of illegitimate behaviors within a multi-robot system.

This paper discusses various soft security considerations that should be accounted for in the next generation of advanced military unmanned systems. These considerations are vital since the unmanned systems will be required to cooperate in highly dynamic, unstructured, and hostile environments, such as urban warzones, natural or man-made disaster areas, and subterranean caves and mines. These systems will also be more autonomous and more common in military operations in the future, and likely have the ability to decide to how they will interact with other robots and humans, given the presence of uncertainty and partial information. Because of all of these challenges, it is essential for these systems to have the ability to quantify trust computationally in observed behaviors of other unmanned systems to ensure productive collaborative and cooperative activities. By using computational trust as a basis for soft security, unmanned systems would have a new ability to evaluate trade-offs between security and performance when dealing with other unmanned systems.

MODELING UNMANNED SYSTEMS AS MANETS

Mobile Ad hoc Networks (MANETs) are groups of mobile agents which can self-configure and form wireless communication networks without the need of a fixed infrastructure or centralized control authority [12] [13]. The MANET lends itself well for modeling teams of unmanned ground systems and allows us to underscore the different types of security vulnerabilities that can be exploited by motivated adversaries.

MANETs, in general, are able to be deployed quickly without any advanced planning for expensive network infrastructure, making them ideal for military applications, emergency rescue operations, and environmental monitoring. Unfortunately, within such a network, it is often difficult to ensure secure communications. Agents are usually susceptible to passive eavesdropping, active interference, data tampering, information leakages, impersonation, and message replay.

In addition to securing communications, MANETs face other difficulties in practice. Namely, agents may have considerable constraints in bandwidth, computing power, and energy [14]. And for military applications in particular, agents may be deployed in harsh or uncontrollable environments, thereby increasing the likelihood of security compromises and agent malfunctions.

Categorizing Attacks in MANETs

Information-based attacks are dominantly considered in the literature for security schemes in MANETs. These attacks are categorized in a number of ways.

Liu et al describe a classification based on passive and active attacks, which characterize attacks by both the nature of the attack and the type of attacker [15]. Passive attacks occur when unauthorized agents gain access to an asset in the MANET but do not modify any content or behavior in the asset. Examples of passive attacks include eavesdropping and traffic flow analysis. Active attacks, on the other hand, occur when unauthorized agents intentionally influence the network in a nefarious manner. This may take the form of modifying or replaying messages, impersonating another agent, or consuming an excess amount of resources in the network.

Attacks can also be categorized by the legitimacy of the agent in the network, which Wu et al described as insider and outsider attacks [16]. An insider attack is done by an agent who is authorized to access a network but uses the network resource in a malicious way. Insiders generally attempt to exploit bugs or poorly configured privileges. Outsider attacks, on the other hand, are initiated by an unauthorized agent who intends to carry out insider attacks through a stolen authorized account.

Levien categorizes attacks in a more general fashion based on the communications graph [17]. Attacks are considered either as edge attacks or node attacks. Edge attacks are constrained in the sense that only one false opinion can be generated for each edge attack. This type of attack can be thought of as creating a false edge within the trust graph. Node attacks are more powerful, however, and amount to a node being impersonated by a malicious node, resulting in the potential for many edge attacks.

Ways of Attacking MANETs

There are numerous ways an attacker can disrupt the functionality of a MANET [18]. We provide a representative, but non-exhaustive, list of attacks against MANETs. This list intends to show the diversity of potential attacks that computational trust schemes may need to defend against to ensure efficient and secure communications.

- **False Recommendation Attack (FRA).** In a FRA, a malicious node provides false recommendations to isolate good nodes from the network. In a similar “stacking attack”, a malicious node keeps complaining about another node to establish a negative reputation for the other node. A trust scheme’s ability to aggregate multiple recommendations from multiple nodes can reduce the influence of such an attack [19].
- **On-Off Attack (OOA).** In an OOA, a malicious node alternates between behaving well and badly, depending on the importance of the situation. Its goal is to stay undetected while disrupting services. Handling this attack can be done by weighting older observations less than newer observations, and aggregating many different observations from multiple sources into a trust scheme to reduce the influence of such an attack.
- **Conflicting Behavior Attack (CBA)**. In a CBA, a malicious node behaves differently to different groups of nodes with the intent to create a conflict between the groups. For example, a malicious node may provide a positive recommendation about a node to one group, but a negative recommendation about the same node to a different group. This results in confusion and non-trusted relationships, which impacts the effectiveness of communications within a

network. A CBA can be handled in much the same way as an OOA.

- **Camouflage Attack**. In a camouflage attack, a malicious node attempts to build up trust by behaving similarly to the observed majority of nodes. Then, after enough trust has been earned, it begins to behave badly for specific occasions. This attack is often difficult to detect, especially if the bad behaviors do not frequently occur or penalties from other nodes are relatively low. Generally, a centralized trust scheme has the best chance of noticing these types of attacks since it has access to all observations about every node in the network.
- **Collusion Attack**. In a collusion attack, multiple malicious nodes collaborate to give false recommendations about good nodes. In this sense, it is very similar to the FRA, but more difficult to defend against. Direct observations of the good node under attack often provide the best defense against collusion attacks; however, because of the mobile nature of MANETs, it may be difficult to maintain vigilance against motivated adversaries.
- **Newcomer / Sybil Attack**. Newcomer and Sybil attacks are similar in the sense that they try to make good nodes misidentify the malicious node, thereby making past trust measurements obsolete. For a newcomer attack, a malicious node attempts to discard its bad reputation by leaving a system and later rejoining it as a 'new user', thereby flushing out its previous history. For a Sybil attack, a malicious node claims and controls multiple identities, and ruins the reputation of the stolen identities. This type of attack affects topology maintenance and fault tolerant schemes, such as multi-path routing. Trust schemes without a centralized administrative node are particularly vulnerable to both types of attacks.

OVERVIEW OF COMPUTATIONAL TRUST

The previous section highlighted security problems related to the uncertainty that comes from interacting with other agents. To address these problems, unmanned systems can use computational trust models, which are designed to give agents the ability to reason about the reciprocity, honesty, and reliability of other agents. Since agents in a system can reasonably be assumed to have selfish interests, these models take the view point of an agent trying to find the most reliable agents to interact with from a pool of potential agents [20].

Computational trust calculations generally take into account some combination of the following three components [21]:

- **Experience**. This component is directly measured by an agent, usually as a result of a direct interaction with a neighboring agent.
- **Recommendations**. This component refers to measurements or trust-based information received from a neighboring agent concerning another agent in the network.
- **Knowledge**. At a minimum, this component includes "common knowledge," which implies that every agent in the system definitely knows the truth about some aspect of their existence. However, it can also incorporate any previously evaluated trust values, measurements, or recommendations.

Trust Definitions, Metrics, and Properties

A universally-accepted definition of computational trust has not been established [22]. This may be due to the abstract nature of trust, but more likely, it is a reflection of the variety of computational models used to estimate trustworthiness. This being said, trust definitions can be broadly segmented into the following categories:

- **Definition based on probability**. Trust defined as a probability measure interprets trust to be the probability that another agent will perform some action within a specific time in a specific context [23] [24] [25] [26].
- **Definition based on belief**. Trust defined as a belief interprets trust as the willingness to act on the basis of another's actions or opinions [27] [28]. These beliefs are generally based on probabilities for related actions and opinions.
- **Definition based on transitivity**. Trust defined as a transitive relationship interprets trust as a weighted binary relation between two members in a network [29].

Trust metrics are used to evaluate and compare trust in different contexts. In every reviewed case, it is regarded as a relative factor that is represented as one of the following:

- **Scaled Value.** Represented as a continuous or discrete value within some range to measure the level of trust [30]. Lower values generally refer to low trust or explicit distrust; high values refer to high trust.
- **Multi-faceted representation.** Represented as a combination of values. For example, a trust metric can be represented as a combination of a trust value and a confidence measure [31]. Another metric represents trust as a triplet of belief, disbelief, and uncertainty [32].
- **Logical metric.** Represented as a value that is a result of some logical or application-specific calculation. Some approaches use probability as a metric [33] [34]. Others use ratios of good and bad results to estimate

trust [35]. Fuzzy logic has also been used to associate labels from natural language to trust values [36].

The literature also describes certain properties of trust that are frequently found in trust networks [18] [22].

- **Dynamicity**. This property says that trust is based on changing temporal and spatial local information, and therefore, is never static.
- **Subjectivity**. This property implies that different trusters can determine different levels of trust against the same trustee due to different private biases, world views, and experiences.
- **Asymmetry**. This property says that trust is unidirectional between agents. So agent i can trust agent j to some level, but agent j does not necessarily need to trust agent i to the same level.
- **Transitivity**. This property implies that trust can be passed along a path of trusting nodes. So if agent i trusts agent j, and agent j trusts agent k, then agent i can trust agent k to a certain level. However, in order to use transitivity between two agents to a third party, a truster must maintain two types of trust: trust in the trustee and trust in the trustee's recommendation of the third party.
- **Composiblity**. This property means that trust information received from all available paths can be composed together to obtain a single trust value.
- **Context-Dependency**. This property provides the meaning behind a trust value by framing it within specific constraints of an agent's abilities or behaviors. For example, a plumber may be trustworthy to fix a clogged water drain, but untrustworthy to perform a triple-bypass heart operation, even though both activities deal with improving fluid flow.

Trust Dynamics

Trust can change and evolve over time in a multi-agent system on the basis of time, agent experience, and data from other information sources. Ultimately, these changes influence the behavior dynamics of each agent. Trust dynamics are generally characterized by the way trust propagates through a network and the way trust is aggregated with other trust-based information.

Trust propagation refers to the mechanism of distributing trust information throughout a network. It reduces re-computations of trust by other nodes and can be extremely useful in applications that lack infrastructure, autonomy, mobility, and resources. Recommendations are considered the simplest form of trust propagation, generally provided directly from a neighbor agent concerning some other agent in the system. This said, multi-hop, multi-path propagation is also found in the literature. For example, Gray et al. propose a trust propagation method based off the small world phenomena, allowing for an authenticating node to be found in relatively few hops [37]. Ballal and Lewis also discuss the concept of trust consensus for collaborative control and show how the propagation of trust through a network can lead to a global asymptotic trust consensus among all agents [38].

Trust aggregation is the mechanism that combines trust values received from multiple sources or paths about a single agent in a particular context. The purpose of this mechanism is to suppress malicious nodes from altering the correct trust value within the network. Common trust aggregation functions include arithmetic mean, weighted mean, and min-max. However, other methods have been proposed as well. For example, Wang and Singh provide an aggregation method using subjective logic within the context of belief functions [39]. Here, the aggregation updates a trust triplet of belief, disbelief, and uncertainty through evidence summation within a belief function. Bachrach et al. proposed a gossip-based aggregation method called "pushsum," which aggregates rumor values from multiple sources after receiving them a sufficient number of times [40].

Aggregation schemes have turned up in some multi-agent applications. For example, Baras et al. calculate aggregate trust values in autonomous agent networks based on the data flow routes between agents [41]. Also Zhang et al. present a framework to secure data aggregation against false data injection in wireless sensor networks. Their method exploits redundancy in gathered data to evaluate the trustworthiness of each sensor [42].

Other types of trust dynamics have also been mentioned in the literature, namely trust prediction, trust mirroring, and trust teleportation [43] [44] [45]. **Trust prediction** describes how an agent can determine trust using the predictions of future behaviors (rather than actual observations) as the basis for the trust calculations. **Trust mirroring** uses a truster agent's perceived similarities with another agent as an indicator of future trust. **Trust teleportation** applies trust derived from an existing trust relationship to new relationships that appear to be similar to the existing relationship.

Trust Models

Computational solutions for dealing with trust-based uncertainty are generally found in the forms of either centralized trust models or decentralized trust models [22]. Centralized trust models assume that at least one "trust agent" is globally available and accessible by all agents in a network. This trust agent may compute the trust values for the entire multi-agent system or help agents in their own trust calculations by providing trust-based information on target agents. The weakness in this type of solution, however, is that the trust agent(s) are single points of failure which can be targeted to massively disrupt the entire trust network. This type of solution also suppresses the subjectivity property of the trust network by assuming that different agents have the same trust-based opinion about the same target.

Decentralized trust models, on the other hand, assume that each agent is the center of their own world and is, therefore, responsible for independently calculating their own trust values for other agents they interact with. This "bottom-up" approach allows for a trust network that is both scalable and fault tolerant. However, the individual agents within the network are potentially more vulnerable to trust-based attacks since it is unlikely that any agent knows the most up-to-date trust values for every other agent in the network. Hence, decentralized trust models often use results from a combination of direct interactions and recommendations about other agents to maintain a reasonably complete picture of the trust network.

USING TRUST IN AUTONOMOUS CONVOYS

Having outlined unmanned system vulnerabilities and computational trust in prior sections, this section discusses the application of soft security within an autonomous convoy. Autonomous convoy operations are expected to be one of the near-term, next-generation applications of unmanned technologies [46] [47] [48]. As such, the autonomous convoy mission presents a relevant and constrained application of a computational trust problem.

The Ground Vehicle Robotics group at U.S. Army TARDEC has developed a trust-based vehicle controller that determines the target velocity vector for a convoy vehicle. The controller uses the RoboTrust model [49] within a high-level decision maker to intelligently switch between low-level vehicle control laws. To decide on the appropriate direction for the desired velocity, the trust-based controller chooses its target according to the following priority: (a) following a trusted leader, (b) leading a trusted follower, and (c) default independent control.

In case (a), if the leader is trusted and in the sensor's range, the vehicle attempts to match the speed of the leader at a preconfigured minimum following distance. In the absence of a trusted leader, the vehicle considers case (b). In this case, if the follower is trusted, but perceived to be unsatisfied with vehicle's leadership, then the vehicle attempts to adjust its own behavior to satisfy the follower. In the absence of both a trusted leader and an unsatisfied trusted follower, the vehicle defaults to case (c). In this case, the vehicle does not follow nor intentionally lead. Rather, it independently drives from waypoint to waypoint along a preplanned path.

Internal simulations of the trust-based controller demonstrated its ability to maintain decentralized convoy string stability and resist "bad" vehicles from stealing "good" vehicles during a convoy mission (Figure 1). In future work, the trust-based controller will be implemented on multiple robotic demonstration platforms and tested in cooperative teaming mission scenarios, such as convoy operations, surveillance, and reconnaissance.

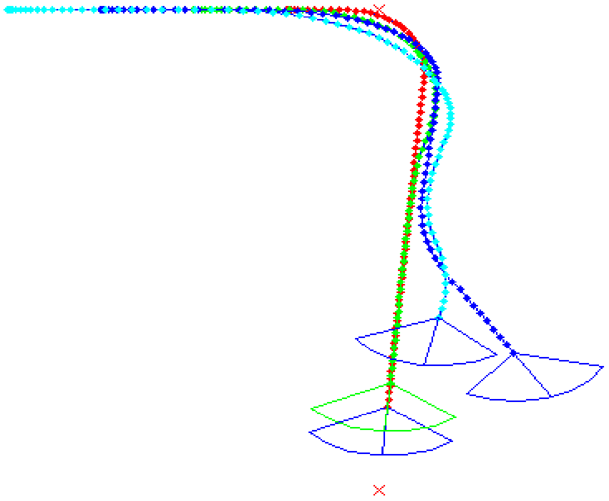

Figure 1: A four-vehicle convoy, in which the blue "bad" vehicle attempts to disrupt the convoy by stealing the cyan "good" vehicle. The path trace shows that the trust-based controller in the cyan vehicle detects the bad behavior of the blue vehicle and disengages its leader-follower control

REFERENCES

[1] "Department of Defense Strategy for Operating in Cyberspace," 2011.

[2] J. Bennett, April 2013. [Online]. Available: http://www.fireeye.com/blog/technical/malware-research/2013/04/the-mutter-backdoor-operation-beebus-with-new-targets.html.

[3] D. Majumdar, December 2011. [Online]. Available: http://www.airforcetimes.com/article/20111209/NEWS/112090311/Iran-s-captured-RQ-170-How-bad-damage-.

[4] N. Shachtman, December 2009. [Online]. Available: http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/.

[5] K. Ziabari, December 2012. [Online]. Available: http://www.globalresearch.ca/another-american-drone-captured-by-iran-washington-feels-trepid/5314601.

[6] P. W. Singer, February 2010. [Online]. Available: http://www.brookings.edu/research/articles/2010/02/22-robot-revolution-singer.

[7] "National Defense Authorization," U.S. Congress, Washington D.C., 2001.

[8] M. Marge, A. Powers, J. Brookshire, T. Jay, O. Jenkins and C. Geyer, "Comparing Heads-Up, Hands-Free Operation of Ground Robots to Teleoperation," in *Robotics: Science and Systems VII*, Los Angeles, 2011.

[9] U.S. Department of Defense, "Unmanned Systems Integrated Roadmap, FY2011-2036," Washington D.C., 2011.

[10] U.S. Department of the Army, "The United States Army Operating Concept, 2016-2028," Washington D.C., 2010.

[11] P. England, Q. Shi, R. J. Askwith and F. Bouhafs, "A Survey of Trust Management in Mobile Ad-Hoc Networks," in *Proc. 13th PGNET*, Liverpool, 2012.

[12] S. Balfe, P. Yau and K. G. Paterson, "A Guide to Trust in Mobile Ad Hoc Networks," *Security and Communication Networks,* vol. 3, no. 6, p. 503–516, 2010.

[13] A. Nasipuri, "Mobile Ad Hoc Networks," in *Wireless Networking,* Oxford, Elsevier, 2008, pp. 423-454.

[14] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," in *RPC 2501 (Informational)*, 1999.

[15] Z. Liu, A. W. Joy and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," in *Proc. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems*, Sushou, 2004.

[16] 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,* pp. 103-135, 2007.

[17] R. Levien and A. Aiken, "Attack-Resistant Trust Metrics for Public Key Certification," in *Proc. 7th USENIX Security Symposium,* San Antonio, 1998.

[18] J. Cho, A. Swami and I. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562-583, 2011.

[19] L. Teacy, J. Patel, N. Jennings and M. Luck, "Coping with Inaccurate Reputation Sources: Experimental Analysis of a Probabilistic Trust Model," in *4th International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS)*, 2005.

[20] S. D. Ramchurn, D. Huynh and N. R. Jennings, "Trust in Multi-Agent Systems," *The Knowledge Engineering Review,* vol. 19, no. 1, pp. 1-25, 2004.

[21] S. Choudhury, S. D. Roy and S. A. Singh, "Trust Management in Ad Hoc Network for Secure DSR Routing," *Novel Algorithms and Techniques in Telecommunications, Automation, and Industrial Electronics,* pp. 496-500, 2008.

[22] K. Govindan and P. Mohaptra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," *IEEE Communications Surveys and Tutorials,* 2012.

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

[24] A. Jøsang, R. Ismail and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems,* vol. 43, no. 2, pp. 618-644, 2007.

[25] A. Jøsang, S. Marsh and S. Pope, "Exploring Different Types of Trust Propagation," *Lecture Notes in Computer Science,* pp. 179-192, 2006.

[26] Y. Wang, C. Hang and M. Singh, "A Probabilistic Approach for Maintaining Trust Based on Evidence," *Journal of Artifical Intelligence Research,* vol. 40, pp. 221-267, January 2011.

[27] C. Castelfranchi and R. Falcone, "Trust is much more than subjective probability: mental components and sources of trust," in *33rd Hawaii International Conference on System Sciences (online edition)*, 2000.

[28] D. J. McAllister, "Affect- and Cognition-based Trust as Foundations for Interpersonal Cooperation in Organizations," *Acadmey of Management Journal*, no. 38, pp. 24-59, 1995.

[29] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," in *Proc. 3rd International Conference on Peer-to-Peer Computing*, Linkoping, 2003.

[30] Y. Ren and A. Boukerche, "Modeling and Managing the Trust for Wireless and Mobile Ad Hoc Networks," in *IEEE International Conference on Communications*, 2008.

[31] G. Theodorakopoulos and J. Baras, "In Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications,* vol. 24, no. 2, pp. 318-328, 2006.

[32] A. Jøsang, "An Algebra for Assessing Trust in Certification Chains," in *Network and Distributed System Security,* San Diego, 1999.

[33] R. Haenni, "Using probabilistic argumentation for key validation in public-key cryptography," *International Journal of Approximate Reasoning,* vol. 38, no. 3, pp. 355-376, 2005.

[34] M. Probst and S. Kasera, "Statistical trust establishment in wireless sensor networks," in *13th International Conference on parallel and Distributed Systems*, 2007.

[35] C. Zouridaki, B. Mark, M. Hejmo and R. Thomas, "Robust cooperative trust establishment for MANETs," in *4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2006.

[36] R. Falcone, G. Pezzulo and C. Castelfranchi, "A fuzzy approach to a belief-based trust computation," in *Lecture Notes on Artificial Intelligence*, 2003.

[37] E. Gray, J. Seigneur, Y. Chen and C. Jensen, "Trust propagation in small worlds," in *1st International Conference on Trust Management*, 2003.

[38] P. Ballal and F. Lewis, "Trust-Based Collaborative Control for Teams in Communication Networks," in *26th Army Science Conference*, Orlando, FL, 2008.

[39] Y. Wang and M. Singh, "Formal Trust Model for Multiagent Systems," in *20th International Joint Conference on Artificial Intelligence (IJCAI),* 2007.

[40] Y. Bachrach, A. Parnes, D. Procaccia and J. Rosenschein, "Gossip-based aggregation of trust in decentralized reputation systems," *Autonomous Agents and Multi-Agent Systems,* vol. 19, no. 2, pp. 153-172, 2009.

[41] J. Baras, T. Jiang and P. Purkayastha, "Constrained Coalitional Games and Networks of Autonomous Agents," in *ISCCSP 2008,* Malta, 2008.

[42] W. Zhang, S. Das and Y. Liu, "A Trust Based Framework for Secure Data Agregation in Wireless Sensor Networks," in *3rd IEEE Communication Society of Sensor and Ad Hoc Communications and Networks*, Reston, VA, 2006.

[43] L. Capra and M. Musolesi, "Autonomic Trust Prediction for Pervasive Systems," in *Proc. 20th International Conference on Advanced Information Networking and Applications,* 2006.

[44] F. M. Ham, E. Y. Imana, A. Ondi, R. Ford, W. Allen and M. Reedy, "Reputation Prediction in Mobile Ad Hoc Networks using RBF Neural Networks," *Engineering Applications of Neural Networks: Communications in Computer and Information Science,* vol. 43, pp. 485-494, 2009.

[45] F. Skopik, D. Schall and S. Dustdar, "Start Trusting Strangers? Bootstrapping and Prediction of Trust," in *Proc. 10th International Conference on Web Information Systems Engineering*, 2009.

[46] D. Green, "Future of Autonomous Ground Logistics: Convoys in the Department of Defense," Fort Leavenworth, KS, 2011.

[47] Robotic Systems Joint Project Office, "Unmanned Ground Systems Roadmap," July 2011. [Online]. Available: http://www.rsjpo.army.mil/images/UGS_Roadmap_Jul11_r1.pdf.

[48] E. Schoenherr, "Moving Future Convoy Operations with Convoy Active Safety Technologies (CAST)," *TARDEC Acclerate Magazine*, vol. 4, pp. 74-78, 2009.

[49] D. G. Mikulski, F. L. Lewis, E. Y. Gu and G. R. Hudas, "Trust Method for Multi-Agent Consensus," in *Proc. SPIE 8387*, Baltimore, 2012.