A SURVEY ON TRUST MANAGEMENT FOR MOBILE AD HOC NETWORKS

K.Seshadri Ramana[1] Dr. A.A. Chari [2] Prof. N.Kasiviswanth[3]

[1]Associate Professor of Dept of MCA Professor, G.Pulla Reddy Engineering College, Kurnool-518002, A.P., India., ramana.kothapalli@gmail.com

[2]Professor Dept of OR&SQC, Rayalaseema University ,Kurnool-518002 ,A.P., India.

3Head Of the Department of CSE, G.Pulla Reddy Engineering College, Kurnool-518002, A.P., India. hodcse@gprec.com

ABSTRACT

Mobile Ad Hoc Network (MANETs) is a Collection of mobile nodes connected with wireless links. MANET has no fixed topology as the nodes are moving constantly form one place to another place. All the nodes must co-operate with each other in order to route the packets. Cooperating nodes must trust each other. In defining and managing trust in a military MANET, we must consider the interactions between the composite cognitive, social, information and communication networks, and take into account the severe resource constraints (e.g., computing power, energy, bandwidth, time), and dynamics (e.g., topology changes, mobility, node failure, propagation channel conditions). Therefore trust is important word which affects the performance of MANET. There are several protocols proposed based on the trust. This paper is a survey of trust based protocols and it proposes some new techniques on trust management in MANETs.

KEY WORDS**:** *Mobile Ad Hoc Networks, Trust Management, Security*.

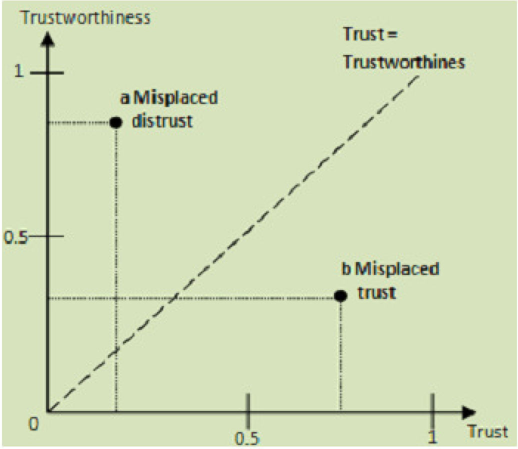
2. ABOUT TRUST

2.1 What is Trust?

The concept of trust is important to communication and network protocol designers where establishing trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. According to Eschenauer et al. [8], trust is defined as “a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities.” According to [7], Trust has also been defined as the degree of belief about the behavior of other entities (or agents).

10.5121/ijnsa.2010.2206

2.2 Relation among Trust, Trustworthiness and Risk



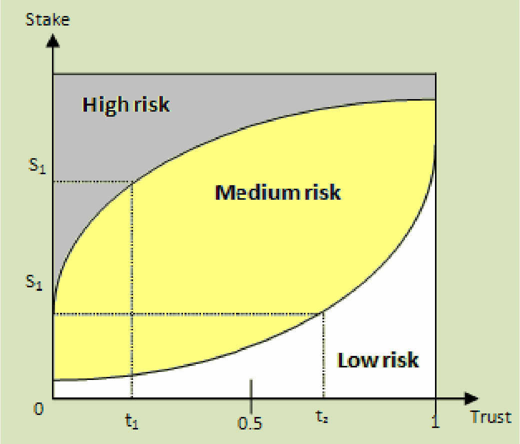


Figure 1: Trust Level

Figure 2: Risk and Trust

In the literature, the terms trust and trustworthiness seem to be interchangeably used without clear distinction. Josang et al. [12] clarified the difference between trust and trustworthiness based on their definitions provided by Gambetta [13]. The level of trust is defined as the belief probability varying from 0 (complete distrust) to 1 (complete trust) [12]. In this sense, trustworthiness is a measure of the actual probability that the trustees will behave as expected. Solhaug et al. define trustworthiness as the objective probability that the trustee performs a particular action on which the interests of the trustor depend. Figure 1 [18] explains how trust (i.e., subjective probability of trust level) and trustworthiness (i.e., objective probability of trust level) can differ and how the difference affects the level of risk the trustor needs to take. In Figure 1, the diagonal dashed line is assumed to be marks of well-founded trust in which the subjective probability of trust (i.e., trust) is equivalent to the objective probability (i.e., trustworthiness). Depending on the extent to which the trustor is ignorant about the difference between the believed (i.e., trust) and the actual (i.e., trustworthiness) probability, there is inconclusiveness about or a miscalculation of the involved risk. That is, the subjective aspect of trust brings incorrect risk estimation and wrong risk management accordingly. Figure 1 shows cases in which the probability is miscalculated. In the area below the diagonal line, there is misplaced trust to various degrees that the perceived trust is higher than the actual trustworthiness. Even though risk is an intrinsic characteristic of trust, even well-founded trust, misplaced trust increases risk and thus the chance of deceit, as shown in the example marked with a and b in Figure 1. On the other hand, when the perceived trust is lower than the actual trustworthiness as shown in the example marked with a, the trustee is distrusted more than warranted. In this case, the trustor may lose potentially good opportunities to cooperate with partners with high trustworthiness.

The relationship between trust and risk has been studied in [12, 18]. Figure 2 shows an example of three different risk values: low, medium, and high. The risk value is low for all trust values when the stake is close to zero. If the stake is too high, risk is regarded as high regardless of the estimated trust value. The risk is generally low when the trust value is high. However, the risk value should be determined based on the value at stake as well as the risk probability; as shown in Figure 2 high risk exists even for the case of trust value = 1. Also important are the aspects (or probability) of opportunity and prospect (or the positive consequence of an opportunity) [12, 18]. The purchaser of rubber should estimate his or her acceptable risk level in terms of the calculated prospects. In general, trust is neither proportional nor inversely proportional to risk.

2.3 Properties OF Trust

Golbeck [9] discusses the three main properties of trust in the context of a social network perspective: transitivity, asymmetry, and personalization. First, trust is not perfectly transitive in a mathematical sense. That is, if A trusts B, and B trusts C, it does not guarantee that A trusts C. Second, trust is not necessarily symmetric, meaning not identical in both directions. A typical example of asymmetry of trust can be found in the relationships between supervisors and employees. Third, trust is inherently a personal opinion. Two people often evaluate trustworthiness about the same entity differently.

2.4 Characteristics of Trust in MANETs

Due to the unique characteristics of MANETs and the inherent unreliability of the wireless medium, the concept of trust in MANETs should be carefully defined. The main features of trust in MANETs are as follows [2, 7, 8, 14, and 19]:

1. A decision method to determine trust against an entity should be fully distributed since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed.
2. Trust should be determined in a highly customizable manner without excessive computation and communication load, while also capturing the complexities of the trust relationship.
3. A trust decision framework for MANETs should not assume that all nodes are cooperative. In resource-restricted environments, selfishness is likely to be prevalent over cooperation, for example, in order to save battery life or computational power.
4. Trust is dynamic, not static.
5. Trust is subjective.
6. Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.
7. Trust is asymmetric and not necessarily reciprocal.
8. Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

3. TRUST MANAGEMENT FOR MANETS

This section surveys existing trust management schemes developed for MANET environments. Before reviewing the literature, we would like to clarify some terminologies that have often been used interchangeably. In general, trust management is interchangeably used with reputation management [16]. However, there are important differences between trust and reputation. Trust is active while reputation is passive [15]. That is, trust is a node's belief in the trust qualities of a peer, thus being extended from a node to its peer. Reputation is the perception that peers form about a node. Also, recommendation is frequently used as a way to measure trust or reputation. Recommendation is simply an attempt at communicating a party's reputation from one community context to another [27, 17].

3.1 Classifications

Trust management is a special case of risk management with a particular emphasis on authentication of entities under uncertainty, and decision making on cooperation with unknown entities [18]. Trust management includes trust establishment (i.e., collecting appropriate trust evidences, trust generation, trust distribution, trust discovery, and evaluation of trust evidence), trust update, and trust revocation [12, 20]. This section introduces popularly used classifications of trust management based on methodologies used for collecting information to evaluate trust.

Li et al. [13] classify trust management as reputation-based framework and trust establishment framework. A reputation-based framework uses direct observation and second-hand information distributed among a network to evaluate other nodes. A trust establishment framework evaluates neighboring nodes based on direct observations while trust relations between two nodes with no prior direct interactions are built through a combination of opinions from intermediate nodes.

Yonfang [25] suggests two different approaches to evaluate trust: policy-based trust management and reputation-based trust management. Policy-based approach is based on strong and objective security schemes such as logical rules and verifiable properties encoded in signed credentials for access control of users to resources. Such a policy-based trust management approach usually makes binary decision according to which the requester is trusted or not, and accordingly the access request is allowed or not. Due to the binary nature of trust evaluation, policy-based trust management has less flexibility. On the other hand, reputation-based trust management utilizes numerical and computational mechanism to evaluate trust. Typically, trust is calculated by collecting, aggregating, and disseminating reputation among the entities.

According to Li and Singhal [16], trust management is classified as evidence-based trust management and monitoring-based trust management. Evidence-based trust management considers anything that proves the trust relationships among nodes including public key, address, identity, or any evidence that any node can generate for itself or other nodes through a challenge/response process. Monitoring-based trust management rates the trust level of each participating node based on direct information (e.g., observing neighboring nodes' benign or malign behaviors such as packet dropping or packet flooding) as well as indirect information (e.g., reputation ratings forwarded from other nodes such as recommendation). Classifications of reputation management schemes may be found in [2] and [25].

3.2 Trust Metrics for MANETs

Even though many trust management schemes have been proposed, no work clearly addresses what should be measured to evaluate trust. Liu et al. [15] define trust in their model as reliability, timeliness, and integrity of message delivery to their intended next-hop. Also most trust-based protocols for secure routing calculate a trust value based on characteristics of well behaving nodes [1, 4, 5, 6, 10, 13, 19, 22, 26]. Trust measurement can be application-dependent and will be different based on the design goals of the proposed network. In this work, we introduce two types of trust based on trust relationships that require measurements of different aspects of trust.

First, social trust refers to properties derived from social relationships. Examples of social networks are strong social relationships such as colleagues or relatives or loose social relationships such as school alumni or friends with common interests [24]. Social trust may include friendship, honesty, privacy, and social reputation/recommendation derived from direct or indirect interactions for “sociable” purpose. In MANETs, some metrics to measure these social trust properties can be frequency of communications, malign or benign behaviors (e.g., false accusation, impersonation), and quality of reputation.

Second, QoS trust represents competence, dependability, reliability, successful experience, and reputation/recommendation on task performance forwarded from direct or indirect interactions with others. In designing network protocols, many prior works measured the trust value of a node based on performance metrics such as the node’s energy or computational power, lifetime, packet delivery rate, or evaluations using reputation or recommendation from other nodes about task performance. The term QoS trust is used in this work to define trust evaluation mainly in terms of task performance capability.

3.3 Existing Trust Management in MANETs

Trust management schemes have been developed for specific purposes such as secure routing, authentication, intrusion detection, and access control (authorization).

Trust Evidence Distribution and Evaluation

Some trust management schemes have been proposed in order to provide a general framework for trust evidence distribution or evaluation in MANETs. Jiang and Baras [20] proposed a trust distribution scheme called ABED (Ant-Based trust Evidence Distribution) based on the swarm intelligence paradigm, which is claimed to be highly distributed and adaptive to mobility. The swarm intelligence paradigm is widely used in dynamic optimization problems (e.g., traveling salesman problem, routing in communication networks) and is inspired from artificial ant colony techniques to solve combinatorial optimization problem. The key principle is called stigmergy, indirect communication through the environment. In ABED, nodes interact with each other through “agents” called ``ants’’ that deposit information called “pheromones”; based on this the agents can identify an optimal path for accumulating trust evidence. However, no specific attacks were considered in [11]. Theodorakopoulos and Baras [20] proposed a trust evidence evaluation scheme for MANETs. The evaluation process is modeled as a path problem in a directed graph where nodes indicate entities and edges represent trust relations. The authors employ the theory of Semirings to show how two nodes can establish trust relationships without prior direct interactions.

Their case study uses the GP web of trust to express an example trust model based on Semirings and shows that their proposed scheme is robust in the presence of attackers. However, their work assumes that trust is transitive. Further, trust and confidence values are represented as binary rather than as a continuous-valued variable. Even though no centralized trusted third party exists, their work makes use of a source node as a trusted infrastructure. Recently Buckerche and Ren [3] proposed a distributed reputation evaluation prototype called GRE (Generalized Reputation Evaluation) to effectively prevent malicious nodes from entering the trusted community. However, no specific attack model was addressed. Further, transitivity, asymmetry, and subjectivity characteristics of trust concept were not specifically explained in building their trust model.

4. TOWARDS TRUST-BASED COGNITIVE MANETS

In this section, we discuss a trust management scheme based on the concept of social and cognitive networks. In addition, we list several issues and questions that developers of MANET trust management schemes should keep in mind.

MANETs pose challenges in designing network security protocols due to their unique characteristics (e.g., resource constraints, vulnerability, unreliable transmission medium, and dynamics). Military MANETs must operate in hostile environments, deal with compromised nodes, support prioritized QoS performance, be able to participate in coalition operations without predefined trust relationships, and facilitate reconfigurability [17]. Thus, additional caution is required in designing security protocols for mission-driven group communication systems (GCSs) in military MANETs

We are particularly interested in evaluating the trust level of such a GCS by evaluating the trust value of a node in terms of its mission execution competence and sociability when a particular mission, X, is assigned. For example, we evaluate each node by asking “Can we trust this group member (node) to do mission X?” That is, our trust management protocol aims to dynamically reconfigure the trust threshold that determines the number of nodes qualified for performing the mission. We take into account the level of risk or difficulty upon failure while considering changing network conditions (i.e., bandwidth, node density, communication rate, degree of hostility) as well as the conditions of participating nodes in the network (i.e., energy, computational power, memory). As a result, the resulting protocols seek to prolong the system lifetime by identifying optimal design settings such as trust value threshold to determine trustable nodes to perform a mission, degree of trust transitivity chains, ratio of trust attributes (i.e., ratio of social trust versus QoS trust, explained in Section 3.2), conditional tolerance threshold of selfish behaviors, and length of trust chains based on efficient tradeoffs made between security and performance properties.

Unlike existing work on trust management in MANETs, our research proposes to embed intelligence in each node with cognitive functionality, adopting recent ideas about cognitive networks in wireless networks [21]. Thomas et al. [21] define a cognitive network first as having a cognitive process that is capable of perceiving current network conditions and then planning, deciding, and acting on those conditions. Cognitive networks are able to reconfigure the network infrastructure based on past experiences by adapting to continuously changing network behaviors to improve scalability (e.g., reducing complexity), survivability (e.g., increasing reliability), and QoS level (e.g., facilitating cooperation among nodes) as a forward looking mechanism [21]. Cognitive networks are also often based on cross-layer design where they share internal information between layers rather than adhering to the traditional strict layered architecture [21].. We propose to use this concept of cognitive networks with cross-layer design for GCS operations in a MANET to introduce cognitive intelligence into each node to adapt to changing network behaviors, such as attacker behaviors, degree of hostility, node disconnection due to physical environment such as terrain, energy exhaustion on a node, or voluntary disconnection for energy savings. We also use social relationships in evaluating the trust metric among group members by employing the concept of social networks. Yu et al. [24] define a social network as a social structure of individuals who may be related directly or indirectly to each other in order to pursue common interests. Yu et al. [24] used social networks to evaluate the overall trust value of a node. However, we use social networks to evaluate the social trust value of a node only in terms of the degree of personal or social trends, rather than the capability of executing a mission based on past collaborative interactions. We assume that a node's capability of completing a highly risky mission will be related to the node's QoS trust value as evaluated by information networks based on information sharing.

Developers of MANET trust management schemes should keep the following questions in mind

- Does the trust metric used reflect the unique properties of trust in MANETs? (e.g., not necessarily perfect transitivity, asymmetry, subjectivity, non-binary value, decaying over time and increasing trust chain, dynamicity, context-dependency)

- What constituents does the trust metric have? Do the constituents change according to tasks given (e.g., high risk upon task failure), changing network environments (e.g., lack of bandwidth, hostile environment as attackers' strength increases, high communication load), or participating nodes' conditions (e.g., low energy, compromised status)?

- How does the trust metric contribute to improving scalability, reconfigurability, and reliability of the proposed network?

- Does the proposed network design achieve adaptability (i.e., learning based on the cognitive functionality of a node) to changing network conditions and environments of MANETs?

- Does the proposed trust metric provide adequate tradeoffs (e.g., altruism versus selfishness, trust level (or security) versus reliability, availability, or survivability, security versus performance)

- Does the proposed network design identify optimal settings under various network and environmental conditions?

5. CONCLUSION

The goal of this paper was to provide MANET network protocol designers with multiple perspectives on the concept of trust, an understanding of the properties that should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the targeted system. By introducing the concept of social and cognitive networks, we suggested future research directions to develop trust management schemes with desirable attributes such as adaptation to environmental dynamics, scalability, reliability, and reconfigurability.

Trust is a multidimensional, complex, and context-dependent concept. Although, trust-based decision making is in our everyday life, trust establishment and management in MANETs faces challenges from the severe resource constraints, the open nature of the wireless medium, the complex dependence between the communications network, the social network, and the application network, and hence the complex dependency of any trust metric to features, parameters, and interactions within and amongst these networks.

REFERENCES:

[1] Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Robust Cooperative Trust Establishment for MANETs," Proc. 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, 30 Oct. 2006, pp. 23-34.

[2]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 (IAW'05), 15-17 June, 2005, West Point, NY, pp. 317-324.

[3]Boukerche and Y. Ren, "A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks," Proc. Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Vancouver, British Columbia, Canada, pp. 88-95, 2008.

[4]S. Buchegger and J. –Y. Le Boudec, "Node Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," Proc. IEEE 10th Euromicro Workshop on Parallel, Distributed, and Network-based Processing, Canary Islands, Spain, Jan. 2002, pp. 403-410.

[5]S. Buchegger and J. –Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks," Proc. 3rd IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing(MobiHOC), Lausanne, CH, 9-11 June 2002, pp. 226-236.

[6]S. Buchegger and J.Y.L. Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems, 15 Nov. 2004.

[7]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.

[8]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.

[9] 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.

[10]T. Ghosh, N. Pissinou, and K. Makki, “Towards Designing a Trust Routing Solution in Mobile Ad Hoc Networks,” Mobile Networks and Applications, vol. 10, pp. 985-995, 2005.

[11]T. Jiang and J. S. Baras, “Ant-based Adaptive Trust Evidence Distribution in MANET,” Proc. 2nd Int’l Conf. on Mobile Distributed Computing Systems Workshops (MDC), Tokyo, Japan, 23-24 March 2004, pp. 588-593.

[12]Josang and S. LoPresti, “Analyzing the Relationship between Risk and Trust,” Proc. 2nd Int’l Conf. Trust Management (iTrust’04), LNCS, Springer-Verlag, 2004, pp. 135-145.

[13]J. Li, R. Li, and J. Kato, “Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks,” IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[14]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. (VTC’07), 22-25 Apr. 2007, pp. 56-60.

[15]J. Liu and V. Issarny, “Enhanced Reputation Mechanism for Mobile Ad Hoc Networks,” Proc. 2nd Int’l Conf. of Trust Management (iTrust 2004), Oxford, UK, March 2004.

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

[17]S. Ruohomaa and L. Kutvonen, “Trust Management Survey,” P. Herrmann et al. (Eds.), iTrust 2005, Lecture Notes in Computer Science, vol. 3477, 2005, pp. 77-92.

[18]Solhaug, D. Elgesem, and K. Stolen, “Why Trust is not proportional to Risk?” Proc. 2nd Int’l Conf. on Availability, Reliability, and Security (ARES’07), 10-13 April 2007, Vienna, Austria, pp. 11-18.

[19]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 Journal on Selected Areas in Communications, vol. 24, no. 2, Feb. 2006, pp. 305-317.

[20]Theodorakopoulos and J. S. Baras, “On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, Feb. 2006, pp. 318-328.

[21]R. W. Thomas, L. A. DaSilva, and A.B. MacKenzie, “Cognitive Networks,” Proc. 1st IEEE Int’l Symposium on New Frontiers in Dynamic Spectrum Access Networks, 8-11 Nov. 2005, pp. 352-360.

[22]Weimerskirch and G. Thonet, “A Distributed Light-Weight Authentication Model for Ad-hoc Networks,” Proc. 4th Int’l Conf. on Information Security and Cryptology (ICISC 2001), 6-7 Dec. 2001.

[23]Yang, H. Luo, F. Ye, S. W. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[24]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.

[25]F. Yunfang, “Adaptive Trust Management in MANETs,” Proc. 2007 Int’l Conf. on Computational Intelligence and Security, Harbin, China, 15-19 Dec. 2007, pp. 804-808.

[26]Zouridaki, B. L. Mark, M. Hejmo and R. K. Thomas, “Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs,” Proc. 3rd ACM Workshop on Security for Ad Hoc and Sensor Networks, Alexandria, VA, Nov. 7, 2005, pp. 1-10.

[27] Abdul-Rahman and S. Hailes, “Using Recommendations for Managing Trust in Distributed Systems,” Proc. IEEE Malaysia Int’l Conf. on Communication (MICC’97), Kuala Lumpur, Malaysia, Aug. 1997.

Authors

K.Seshadri Ramana[1] has completed Master Of Computer Application from Kuvempu University, M.Phil from Annamali University, Chennai and presently doing PhD in Computer Science from Rayalaseem University, Kurnool. He has 10+ years of teaching experience. He published 2 papers in International Journals, two papers in International and National conferences. Presently he is working as Associate Professor in MCA Department, G.Pulla Reddy Engineering College (Autonomous) Kurnool, and A.P.

Dr. .A. ANANDA RAJA CHARI [2] working as Professor & Director of Research in Rayalaseema University, Kurnool. He has 32+ years of teaching experience. He was successfully guided THREE Ph.D research students and ONE student for M. Phil. Degree. Six Ph.D. Students are in the Pipe line and TWO M .Phil. students work is under progress. His Published 21 Research papers in National and International Journals and presented 18 research papers in National and International Conferences in the area of Reliability modeling, Optimization and statistical Quality Control and statistical Inference. He Served as Referee for the JOURNAL OF INSTITUTE OF ELECTRICAL AND ELECTONICS ENGINEERING TRANSACTIONS IN RELIABILITY (IEEE), A Journal of ASQC association, North Carolina, USA. Served as member of the INTERNATIONAL Advisory Committee in organizing an FIRST International Conference on Quality , Reliability and IT (ICQRIT)- 2003 Jointly organized by Dept. of Operations Research , University of Delhi, DRDA New Delhi & IIT Bombay during 18-20 , Dec, 2003 at the Indian National Science Academy, New Delhi. Serving as member of the INTERNATIONAL Advisory Committee in organizing SECOND & third International Conference on Quality , Reliability and IT (ICQRIT)- 2005 & 2006 Jointly organized by Dept. of Operations Research , University of Delhi, DRDA New Delhi & IIT Bombay at Indian National Science Academy, New Delhi.

Prof.N.Kasiviswanath[3] has completed B.E in Computer Science & Engineering from Marathwada University, M.S from Birla Institute of Technology & Science, Pilani and recently submitted the research thesis for the award of PhD in Computer Science.. He has 17+ years of teaching experience. He published 10 papers in National and International Journals, 2 International and 6 National conferences. Presently he is working as Professor & Head of CSE Department, G.Pulla Reddy Engineering College, Kurnool, A.P, INDIA. He was the author of Text book on “Data Structures through C++”, M/s Laxmi Publications, New Delhi. He is also the Chairman of Board of Studies in Computer Science and Information Technology for Sri Krishna Devaraya University and G.Pulla Reddy Engineering College (Autonomous), Kurnool.