Review Paper on Calculation, Distribution of Trust & Reputation in MANET

Swapnali Sundar Sadamate, V. S. Nandedkar

Abstract- This paper is Review on Managing trust in a distributed Mobile Ad Hoc Network (MANET) Which is a challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability, availability, scalability, and reconfigurability. 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. We provide a survey of trust management schemes developed for MANETs and discuss generally accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs. Finally, we discuss future research areas on trust management in MANETs based on the concept of social and cognitive networks.

Index terms- MANET, Security, Trust

I. INTRODUCTION

In an increasingly networked world, increased connectivity could lead to improved information sharing, facilitate collaboration, and enable distributed decision making, In mobile ad hoc networks (MANETs), the distributed decision making should take into account trust in the elements: the sources of information, the processors of information, the elements of the communications network across which the information is transmitted, etc. This trust must often be derived under time-critical conditions, and in a distributed way. Due to the mobility of MANETs, most nodes are supposed to be as small as possible to be carried out or to be easy to install in hostile places. However, it is also true that a node may easily be stolen and become compromised. Thus, the trust between nodes in ad-hoc networks cannot be guaranteed. Furthermore, this problem may increase the chance to tamper the stolen node. It is also vulnerable since every node in MANET uses radio wave to communicate. It is very hard to detect any node since there is no explicit evidence. In order to enforce cooperation within the networks, adjacent nodes should build up trust over time. Such trust establishment procedure can improve security, connectivity, and quality of service in the network so that performance is improved. It gives study related to depicts some related work in introducing trust and security in MANETs, describes the work on the theory of trust formalization, illustrates proposed node-based trust management (NTM) scheme Finally depicts the analytical part of NTM with the system architecture and some algorithms.

II. HISTORY

In paper “Future Trust Management Framework for Mobile Ad Hoc Networks “ by Jie Li and Ruidong Li, University of Tsukuba Jien Kato, Nagoya University 2008, they stated the trust management framework, which evaluates the trust of participating nodes, which used to force nodes to cooperate in a normal way. Reputation based frameworks suffer from some possible attacks such as bad mouthing, on-off, conflicting behavior, sybil, and newcomer attacks. In addition, in a reputation-based framework the confidence *value*, which is an important parameter characterizing the statistical reliability of the computed trust, has not been considered. The existing trust establishment frameworks also suffer from the attacks mentioned for reputation-based frameworks. On the other hand, a trust establishment framework is known to be vulnerable under a novel selective misbehavior attack in this article. By this type of attack, the attacker aims to exclude victim nodes from a network and meanwhile makes itself able to obtain normal service from the network.

To solve the above mentioned vulnerabilities with existing trust management frameworks, they designed a robust and attack-resistant framework, which is called the objective trust management framework (OTMF).

In paper “A TRUST-BASED SECURITY ARCHITECTURE FOR TACTICAL MANETS” by Yannick Lacharité, Dang Quan Nguyen, Maoyu Wang, and Louise Lamont Communications Research Centre Canada (2008), they presented a general architecture for a security trust monitoring layer that runs on top of routing protocols. This security layer can be applied to different MANET routing protocols and provide monitoring of different network attacks by adding specific plug-ins. Our modular security approach allows nodes, running different routing protocols and equipped with different security

solutions, to inter-operate by exchanging security information with each other. The idea is to have a security layer monitor MANET communications and construct a trust representation model of member nodes of the MANET. The trust information gathered can be communicated to MANET nodes (upon request), and such nodes can modify their routing tables accordingly. Then they provided the design overview of the Security Trust Monitor (STM) concept in that STM’s design is integrated with an OLSR plug-in to better explain the Relationship between the network and “security” layers.

In paper “Cryptographic Versus Trust-based Methods for MANET Routing Security” by Jared Cordasco Susanne Wetzel in which they have given the first comparison of SAODV and TAODV, two MANET routing protocols,

Manuscript Received on May 2013.

Miss. Swapnali Sundar Sadamate, Department of Computer Engineering Padmabhooshan Vasantdada Patil Institute of Technology, Bavdhan, Pune-21, India

Prof. Mrs. V.S.Nandedkar, Department of Computer Engineering Padmabhooshan Vasantdada Patil Institute of Technology, Bavdhan, Pune-21, India

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

which address routing security through cryptographic and trust-based means respectively. They provided performance comparisons on actual resource-limited hardware.

In paper “Trust Based Malicious Nodes Detection in MANET” by Wei Gong1,2, Zhiyang You1,2, Danning Chen2, Xibin Zhao2, Ming Gu2, Kwok-Yan Lam2(2009), they Node misbehavior due to selfish or malicious intention could significantly degrade the performance of MANET because most existing routing protocols in MANET are aiming at finding most efficiency path. To deal with misbehavior in MANET, an incentive mechanism should be integrated into routing decision making. In this paper firstly we review existing techniques for secure routing, and then propose to use trust vector model based routing protocols. Each node would evaluate its own trust vector parameters about neighbors through monitoring neighbors’ pattern of traffic in network. At the same time, trust dynamics is included in term of robustness. Then they evaluated the performance of the proposed mechanism by modifying Dynamic Source Routing (DSR).

In paper “DualTrust: A Trust Management Model for Swarm-Based Autonomic Computing Systems” by WM Maiden (May 2010), he said that certain characteristics of the mobile agent ant swarm – their lightweight, ephemeral nature and indirect communication – make the design of a trust management model for them especially challenging. This thesis examines the trust relationships, issues, and opportunities in a representative system, assesses the applicability of trust management research as it has been applied to architectures with similar characteristics, and finds that by monitoring the trustworthiness of the autonomic managers rather than the swarming sensors, the trust management problem becomes much more scalable and still serves to protect the swarm. This thesis then proposes the DualTrust conceptual trust model. autonomic manager’s bi-directional primary relationships in the ACS architecture, DualTrust is able to monitor the trustworthiness of the autonomic managers, protect the sensor swarm in a scalable manner, and provide global trust awareness for the orchestrating autonomic manager.

III. OVERVIEW

CONCEPTS AND PROPERTIES OF TRUST- Here we review how trust is defined in different disciplines and how these trust concepts can be applied in modeling trust in MANETs. Further, we examine the relationship between trust and risk.

A. Multidisciplinary Concept of Trust-

According to Merriam Webster’s Dictionary, trust is defined as ”assured reliance on the character, ability, strength, or truth of someone or something.” Despite the subjective nature of trust, the concept of trust has been very attractive to network security protocol designers because of its diverse applicability as a decision making mechanism.

Trust in sociology:

Gambetta describes the nature of trust as subjectivity, an indicator for future actions, and dynamicity based on continuous interactions between two entities. Luhmann also emphasized the importance of trust in society as a mechanism for building cooperation among people to extend human interactions for future collaboration. Adams et al. Represented trust as a continuous variable, quantifying trust in the light of context or acceptance of risk. They further stressed that risking betrayal is an important aspect in building trust.

Trust in economics:

In economics, trust is represented as an expectation that applies to situations in which trustors take risky actions under uncertainty or information incompleteness.

Trust in philosophy:

According to the Stanford Encyclopedia of Philosophy, trust is important but dangerous. Since trust allows us to form relationships with others and to rely on others for love, advice, help, etc., trust is regarded as a very important factor in our life that compels others to give us such things with no outside force such as the law. On the other hand, since trust requires taking a risk that the trustee may not behave as the trustor expects, trust is dangerous implying the possible betrayal of trust.

Trust in psychology:

According to the Wikipedia definition of trust in psychology, trust starts from the birth of the child. As the child grows older, trust also grows stronger. However, the root of trust derives from the relationship between mother (or caregiver) of the child since the strength of the family relies on trust, if the child is raised in a family which is very accepting and loving, the child also returns those feelings to others by trusting them. But if trust is lost, it is hard to regain it.

Trust in organizational management:

In this field, the concept of trust is also defined as the extent to which one party is willing to count on someone or something with a feeling of relative security in spite of possible negative consequences, emphasizing the possibility of facing. Trust concepts in organizational management can give us insights on how to measure trust by investigating methods to measure ability, integrity, and benevolence of each networked node, as well as on assessing risk.

Trust in autonomic computing:

As technology becomes more complex, fully understanding automation becomes infeasible, if not impossible, and trust in automation becomes critical, particularly when unexpected situations arise and system responses cannot be predicted. Lee and See define trust as the attitude that an agent will help accomplish an individual’s goals in a situation with uncertainty and vulnerability.

Trust in communications and networking:

The concept of trust also has been attractive to communication and network protocol designers where trust relationships among participating nodes are critical in building cooperative and collaborative

environments to optimize system objectives in terms of scalability, reconfigurability, and reliability (i.e., survivability), dependability, or security

Trust metric having the following characteristics:
(1) trust should be established based on potential risks;
(2) trust should be context-dependent;
(3) trust should be based on each party's own interest (e.g., selfishness);
(4) trust is learned (i.e., a cognitive process); and
(5) trust may represent system reliability.

Trust, Trustworthiness, and Risk- The terms trust and trustworthiness seem to be used interchangeably without clear distinction. Josang et al.clarified the difference between trust and trustworthiness based on definitions provided by Gambetta ,Level of trust is defined as the belief probability varying from 0 (complete distrust) to 1 (complete trust). In this sense, trustworthiness is a measure of the actual probability that the trustees will behave as expected.

There are two interesting types of trust:
1) a context independent reliability trust which measures the perceived reliability by another party regardless of the situations which the trustor might face by recognizing possible risk;
2) decision trust as "the extent to which a given party is willing to depend on something or somebody in a given situation with a feeling of relative security even though negative consequences are possible."
Decision trust deals with components such as utility and risk attitude. As an example, one may not trust an old rope for climbing down from the 3rd floor of a building during a fire exercise (i.e., reliability trust) while trusting the rope in a real fire (i.e., decision trust). Trust Properties in MANETs- The main properties of trust in MANET environments can be summarized as follows (see Figure 1):

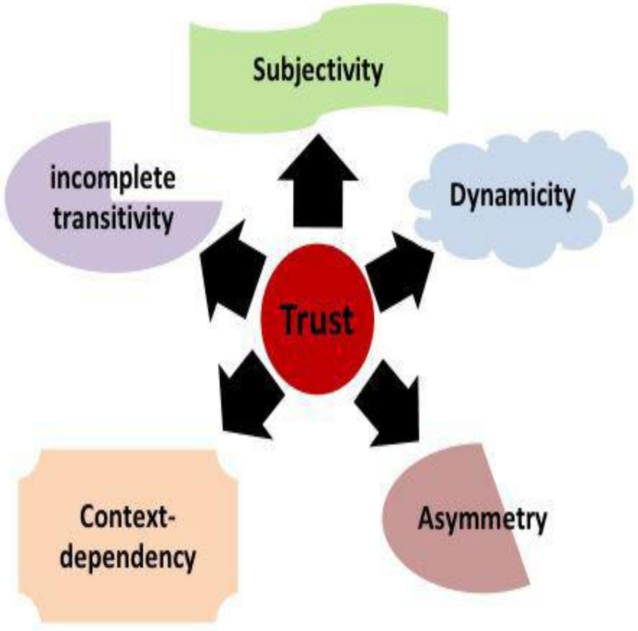

Fig. 1. Trust properties in MANETs.

1. dynamic, not static-Trust establishment in MANETs should be based on temporally and spatially local information: due to node mobility or failure, information is typically incomplete and can change rapidly. Adams et al. point out that in order to capture the dynamicity of trust, trust should be expressed as a continuous variable, rather than as a binary or even discrete-valued entity. A continuous valued variable can represent uncertainty better than a binary variable.

2. trust is subjective- In MANET environments, a trustor node may determine a different level of trust against the same trustee node due to different experiences with the node derived from a dynamically changing network topology.

3. trust is not necessarily transitive- For example, if A trusts B, and B trusts C, it does not guarantee A trusts C. In order to use the transitivity of trust between two entities to a third party, a trustor should maintain two types of trust: trust in a trustee and trust in the trustee's recommendation of the third party.

4. trust is asymmetric not necessarily reciprocal- In heterogeneous MANETs, nodes with higher capability may not trust nodes with lower capability at the same level that nodes with lower capability trust nodes with higher capability. Example in organizational management, a supervisor tends to trust an employee less than the employee trusts the supervisor.

5. trust is context-dependent- For example, A may trust B as a wine expert but not as a car fixer. Similarly in MANETs depending on the given task, different types of trust (e.g., trust in computational power or trust in unselfishness, trust in forwarding versus trust in reporting) are required.

In order to properly take into account these unique characteristics of trust in MANETs as described above, any trustbased framework for MANETs should consider the following as well:

First, a decision procedure to determine the trust of an entity should be fully distributed based on cooperative evaluation with uncertain and incomplete evidence, since one cannot rely on a trusted third party such as a trusted centralized certificate authority to take care of trust management as in wired networks.

Second, trust should be determined in a highly customizable way (e.g., flexible to membership changes and to deployment scenarios) without causing disruption to the device computation and communication resources while capturing the various and complicated natural components of an individual's trust into a network model.

Third, a trust decision framework should not assume that all nodes are cooperative. Finally, trust should be established in a self-organized reconfigurable way in order not to be disrupted by the dynamics of MANET environments. In addition to the characteristics mentioned above, trust-based frameworks for MANETs should consider the tradeoff issues between security and performance including reliability, fault tolerance, scalability, and energy consumption where resources are restricted but security vulnerability is relatively high.

IV. CLASSIFICATIONS, POTENTIAL ATTACKS, AND METRICS FOR MANET TRUST MANAGEMENT

According to Liu et al., trust is active while reputation is passive. 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. Further, Ruhomaa et al. distinguish trust from reputation, noting that trust puts an emphasis on risk and incentives while reputation focuses on a perception that a party creates through past actions about its intentions in the context of the norms effective within a community.

A. Classifications-

According to Solhaug et al, 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. However, the application of trust management has been extended from authentication to various aspects of communications and networking, including secure routing for isolating malicious or selfish nodes, intrusion detection, key management, access control, and other decision making mechanisms. Trust management includes trust establishment (i.e., collection of appropriate trust evidence, trust generation, trust distribution, trust discovery, and evaluation of trust evidence), trust update, and trust revocation. Yonfang suggests two different approaches to evaluate trust: policy-based trust management and reputation-based trust management.

Based trust management 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. In addition, the access decision is usually on the basis of mechanisms having a well defined trust management language that has strong verification and proof support. Such a policy-based trust management approach usually makes a 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. Furthermore, the availability of (or access to) trusted certificate authorities (CA) cannot always be guaranteed, particularly for distributed systems such as MANETs.

On the other hand, Reputation-based trust management utilizes numerical and computational mechanisms to evaluate trust. Typically, in such a system, trust is calculated by collecting, aggregating, and disseminating reputation among the entities. According to Li and Singhal [11], trust management can be classified as evidence-based trust management and monitoring-based trust management.

Evidence-based trust management considers anything that proves trust relationships among nodes: these could include public key, address, identity, or any evidence that any node can generate for itself or other nodes through a challenge and response process.

Monitoring based trust management rates the trust level of each participating node based on direct information (e.g., observing the benign or malicious behaviors of neighboring nodes, such as packet dropping, and packet flooding leading to excessive resource consumption in the network, or denial of service attacks) as well as indirect information (e.g., reputation ratings, such as recommendations forwarded from other nodes).

Aivaloglou et al. [12] classify two types of trust establishment frameworks for MANETs: certificate-based framework versus behavior-based framework. In the former, mechanisms are defined for pre-deployment knowledge of trust relationships within the network, using certificates which are distributed, maintained and managed, either independently or cooperatively by the nodes. Trust decisions can be made based on a valid certificate that proves trustworthiness of the target node by a certificate authority or by other nodes that the issuer trusts.

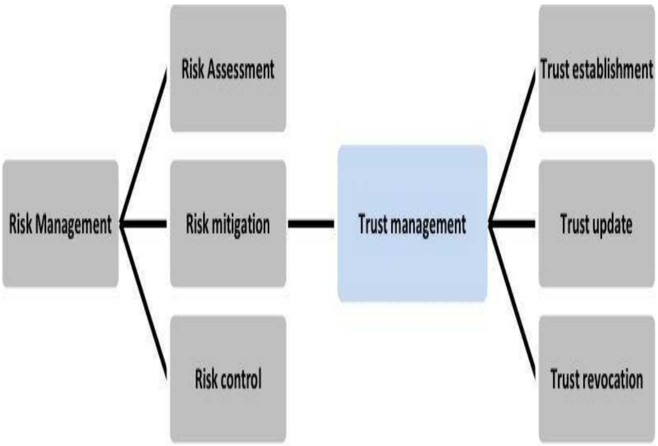

Fig. 2. Definition of trust management.

In behavior-based framework, each node continuously monitors behaviors of its neighboring nodes in order to evaluate trust. The behavior-based framework is a reactive approach, operating under the assumption that the identities of nodes in the network are ensured by preloaded authentication mechanisms. For example, if a node uses network resources in an unauthorized way, it will be regarded as a selfish or malicious node, and will finally be isolated from other nodes.

Aivaloglou et al. also classify trust establishment schemes in terms of the type of architectures used: hierarchical framework versus distributed framework. In the former, a hierarchy exists among the nodes based on their capabilities or levels of trust. In this framework, centralized certificate authorities or trusted third parties are usually provided for on-line or off-line evidence. Such a centralized infrastructure does not exist in a distributed framework; hence, each node has some, possibly equal, responsibility for acquiring, maintaining, and distributing trust evidence.

Adams et al. propose three types of reputation systems: positive reputation, negative reputation, and a combination of the two. Positive reputation systems only consider observations or feedback of the positive behaviors of a node. Negative reputation systems only record complaints or observations of the negative behaviors of a node. Peers are assumed to be trusted and so feedback on behaviors is used to negatively reflect a node’s reputation. To complement the drawbacks of these mechanisms, hybrid reputation systems have been proposed.

B. Potential Attacks-

One classification of attacks is passive attack versus active attack. A passive attack occurs when an unauthorized party gains access to an asset but does not modify its content. Passive attacks include eavesdropping and traffic analysis (e.g., traffic flow analysis).

Active attacks usually take the form of one of the following four types or combinations: masquerading (i.e., impersonation attack), replay (i.e., retransmitting messages), message modification, and denial-of-service (DoS) (leading to excessive resource consumption in the network).

Specific attack examples:

• Routing loop attacks: A malicious node may modify routing packets in such a way that packets traverse a cycle and so do not reach the intended destination.

• Wormhole attacks: A group of cooperating malicious nodes can pretend to connect two distant points in the network with a low-latency communication link called a wormhole link, causing disruptions in normal traffic load and flow.

• Blackhole attacks: A malicious node, the so called black hole node, may always respond positively to route requests even when it does not have proper routing information. The black hole can drop all packets forwarded to it .

• Grayhole attacks: A malicious node may selectively drop Packets as a special case of a black hole attack. For example, the malicious node may forward routing packets but not data packets. Similarly, a sinkhole attacker attracts nodes to route through it and then selectively routes packets.

• DoS attacks: A malicious node may block the normal use or management of communications facilities, for example, by causing excessive resource consumption.

• False information or false recommendation: A malicious node may collude and provide false recommendations information to isolate good nodes while keeping malicious nodes connected. In the stacking attack, a malicious node keeps complaining about a peer node and creates the peer's negative reputation.

• Incomplete information: A malicious node may not cooperate in providing proper or complete information. Usually compromised nodes collude to perform this attack. However, node mobility or link failure, prevalent in MANETs, may also result in the same phenomenon.

• Packet modification/insertion: A malicious node may modify packets or insert malicious packets such as packets with incorrect routing information.

• Newcomer attacks: A malicious node may discard its bad reputation or distrust by registering as a new user. The malicious node simply leaves the system and joins again for trust revocation, flushing out its previous bad history and starting to accumulate new trust.

• Sybil attacks: A malicious node can use multiple network identities which can affect topology maintenance and fault tolerant schemes such as multi-path routing.

• Blackmailing: A malicious node can blackmail another node by disseminating false information that another node is malicious or misbehaving. This can generate significant amount of traffic and ultimately disrupt the functionality of the entire network. This attack can be seen as false accusation plus DoS attacks in the sense that false information is disseminated leading to a significant amount of resource consumption.

• Replay attacks: A malicious node may replay earlier transmitted packets. If the packets include data, this should not cause trouble, and the receiving node just discards erroneous packets. However, if the adversary replays route requests, routing table information would become erroneous, and old locations and routing information might make nodes unreachable.

• Selective misbehaving attacks: A malicious node behaves badly but selectively to other nodes.

• On-off attacks: A malicious node may alternatively behave well and badly to stay undetected while disrupting services.

V. CONCLUSION

Trust is not a constant value, it changes over time. Trust between nodes is important to perform functions of the network. Trust management is necessary when nodes participating with each other to perform certain actions. Trust management framework evaluates trust among nodes in the network and then form trust relations between them. Trust based methods have advantages over Cryptographic mechanism. Trust management helps to detect and isolate malicious node in the network. Trust management framework should be designed to detect malicious nodes in the MANET's and it can take help of trust metrics and we can use social terms like honesty, friendship to manage the trust in network. To manage the trust in the network, incentives and punishment strategy can be used for good and misbehavior of nodes respectively.

FUTURE WORK

The important directions for future work are

1. Impact of network dynamics on trust
2. Computations of trust in cooperative and non cooperative games
3. Impact of heterogeneous nodes on trust
4. Security paradigms to enhance trust in the network
5. Social and context dependent trust

REFERENCES

1. Jin-Hee Cho; Swami, A.; Ing-Ray Chen;"A Survey on Trust Management for Mobile Ad Hoc Networks", Communications Surveys Tutorials, IEEE , vol.13, no.4, pp.562-583, Fourth Quarter 2011.
2. Jared Cordasco1, Susanne Wetzel1;"Cryptographic Versus Trust-based Methods for MANET Routing Security," 2008.
3. Jie Li; Ruidong Li; Jien Kato; "Future trust management framework for mobile ad hoc networks," Communications Magazine, IEEE , vol.46, no.4, pp.108-114, April 2008.
4. Lacharite, Y.; Dang Quan Nguyen; Maoyu Wang; Lamont, L.; "A trust-based security architecture for tactical MANETS," Military Communications Conference, 2008. MILCOM 2008. IEEE, vol., no., pp.1-7, 16-19 Nov. 2008.
5. Wei Gong; Zhiyang You; Danning Chen; Xibin Zhao; Ming Gu; Kwok-Yan Lam;" Trust Based Malicious Nodes Detection in MANET", E-Business and Information System Security, 2009. EBISS '09. International Conference on, vol., no., pp.1-4, 23-24 May 2009.
6. Govindan, K.; Mohapatra, P.;"Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", Communications Surveys Tutorials, IEEE , vol.PP, no.99, pp.1-20, 0.
7. Raihana Ferdous, Vallipuram Muthukkumarasamy, Abdul Sattar;"Trust Management Scheme for Mobile Ad-Hoc Networks ", 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).
8. A. A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks," *Wireless Personal Communications*, vol. 37(1-2), pp. 139–168, 2006

9. S. Buchegger and J. L. Boudec, “A robust reputation system for P2P and mobile ad-hoc networks,” in *In Proc. 2nd Workshop on Economics of Peer-to-Peer Systems*, 2004.
10. Z. Liu, A. W. Joy, and R. A. Thompson, “A dynamic trust model for mobile ad hoc networks,” in *IEEE International Workshop on Future Trends of Distributed Computing Systems, FTDCS’04*, pp. 80–85, May 2004.
11. M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, “Quantifying trust in mobile ad-hoc networks,” in *International Conference on Integration of Knowledge Intensive Multi-Agent Systems*, pp. 65–70, April 18-21, 2005.
12. S. S. Park, J. H. Lee, and T. M. Chung, “Cluster-based trust model against attacks in ad-hoc networks,” in *Third International Conference on Convergence and Hybrid In63formation Technology*, pp. 526–532, 2008.
13. D. Quercia, S. Hailes and L. Capra, “Lightweight distributed trust propagation,” in *The Seventh IEEE International Conference on Data Mining*, pp. 282–291, 2007.