Cognitive security management with reputation based cooperation schemes in heterogeneous networks

Conference Paper · May 2009

DOI: 10.1109/CICYBS.2009.4925085 · Source: IEEE Xplore

7 authors, including:

Minsoo Lee
LG Electronics
36 PUBLICATIONS **240** CITATIONS
SEE PROFILE

Xiaohui Ye
University of California, Davis
25 PUBLICATIONS **595** CITATIONS
SEE PROFILE

Samuel Johnson
University of North Texas
32 PUBLICATIONS **369** CITATIONS
SEE PROFILE

Dan Marconett
University of California, Davis
11 PUBLICATIONS **151** CITATIONS
SEE PROFILE

Cognitive Security Management with Reputation based Cooperation Schemes in Heterogeneous Networks

Minsoo Lee, *Member, IEEE*, Xiaohui Ye, *Student Member, IEEE*, Samuel Johnson, Dan Marconett, *Student Member, IEEE*, Chaitanya VSK, Rao Vemuri, *Senior Member, IEEE*, and S. J. Ben Yoo, *Fellow, IEEE*

***Abstract*— This paper proposes a Computational Intelligence framework for network security management. The framework uses reinforcement learning and Bayesian methods to achieve cross-layer optimization in heterogeneous, multi-layer wireless and wireline networks. Metrics based on the reputation of a node are used to measure performance. OPNET simulations results indicate that routing algorithms based on the newly proposed framework exhibit nearly four times improved network performance measured in terms of goodput.**

I. Introduction

Mobility and dynamic reconfiguration requirements under adverse environmental conditions call for adaptive, cognitive networking concepts. Therefore, the network nodes should employ *situation awareness* to determine the existence of abnormal events in their surroundings [1]. One particular bottom-up approach enabling situation awareness involves the application of a *reputation system* in which the network nodes establish trust and form opinions based on one another's observed performance and behavior. For proper assessment of node cooperation in communication systems, incentive mechanisms (pricing mechanisms as well as rules) and artificial immune systems [2, 3] have been investigated. Other security challenges often incurred are malicious attacks and random failures. Collaborative filtering [4] and reputation systems [5-8] address both these issues as well as incentives. Here, nodes keep track of their peers' behavior through direct observation, cooperative joint observations with other nodes, and opinion exchanging in order to compute a reputation value of their peers. Reputation values are then used to decide with whom to cooperate and which nodes to avoid, i.e. nodes with a good reputation are selected to forward packets. Toward this end, nodes monitor each other, allowing them to identify and isolate misbehaving (potentially compromised) network elements. Second-hand opinions from non-adjacent neighbors are processed using a transitive relationship. Once reputation is calculated, nodes can be classified and management policies enforced.

We propose a reputation system based on Bayesian reputation computation in which nodes combine their individual, partial first-hand observed data with second-hand information of two-hop neighbors in order to develop more complete situation awareness. Our preliminary experimental studies apply the reputation system to a networking scenario in which nodes detect malicious relay nodes which drop or manipulate packets. A routing algorithm was created to consider the reputation of the next-hop nodes during path selection. The simulations reveal that this fusion of a reputation system with a routing algorithm can find alternative paths by avoiding malicious nodes resulting in nearly 4 times higher goodput.

The authors are with Department of Electrical and Computer Engineering, University of California Davis, Davis, CA 95616, (e-mail: msolee@ucdavis.edu, xye@ucdavis.edu, samjohnson@ucdavis.edu, dmarconett@ucdavis.edu, svadrevu@ucdavis.edu, rvemuri@ucdavis.edu, sbyoo @ucdavis.edu)

II. Reputation System for Situation-awareness

A. Proposed Reputation System in a Bayesian Approach

The proposed reputation system is based on the Bayesian reputation framework [9] and consists primarily of two parts: nodes forming opinions of other nodes around certain performance characteristics, and nodes establishing trust relationships between each other. The collective opinions toward a given node constitute the node's reputation. The Bayesian reputation computations take as input the number of positive and negative observations taken over some time period. These values are then used to update the beta probability density function, $beta(\alpha, \beta)$. To illustrate, let s be the ratio of positive observations and $s' = 1 - s$ be the ratio of negative observations over a given time period. The parameters of the PDF are updated such that $\alpha = u \cdot \alpha + s$ and $\beta = u \cdot \beta + s'$, where u is a weight. The beta distribution can be applied to both forming opinions and forming trust. Trust is initially formed between adjacent nodes with first-hand information about each other. Then, if the trust between a pair of nodes is adequate, the two can reinforce their individual opinions about a third-party node with the opinion of the other. Here, what is effectively happening is a node is using second-hand information to further develop its own opinions. Trust allows nodes to exchange and reinforce each other's opinions. This exchange of opinions is an exchange of a combination of first hand observations synthesized with pre-processed second-hand information. Still another way for nodes to assist each other in the process opinion development is to collaborate to collect additional raw "first-hand" information. The need for collaboration arises from the limited quantity and quality of first-hand observations that can be made individually. With collaboration, nodes can combine their individual, partial

978-1-4244-2769-7/09/$25.00 ©2009 IEEE

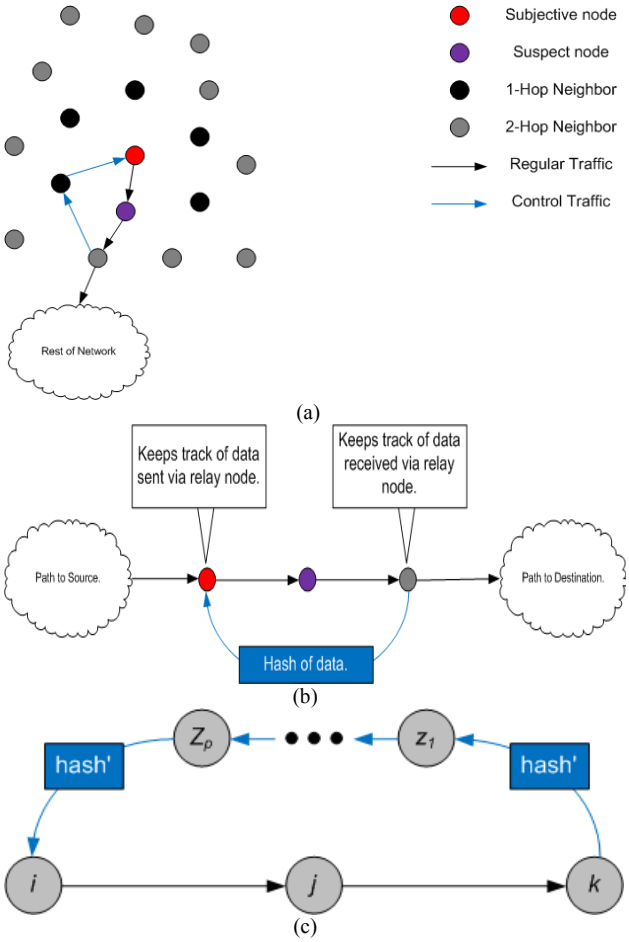


Fig. 1. Reputation building with help from 2-hop neighbors (a) the subjective node and its two-hop neighbors collaborate to characterize the behavior of the one-hop neighbors. (b) 2-hop neighbor feedback of hash data for second hand reputation (c) Bayesian Belief Network based on feedback of hash data

first-hand observed data in order to develop more complete situation awareness.

B. Reputation Building with Help from 2-hop Neighbors

A two hop neighbor sends a feedback packet to the sender node by a secondary routing path (Fig. 1). The feedback packet includes a hash value of received packets and is encrypted by the sender's public key. Public keys are distributed in a P2P manner by multipath. An illustrative example in which such collaboration is applicable is when the two nodes immediately upstream and downstream of a relay node collect and compare data concerning the relay node's behavior with respect to dropping packets or manipulating the packets payload. The upstream node will then be able to determine whether or not the relay node is behaving mischievously; something that it would have been unable to determine independently.

C. Experimental results

In preliminary experimental studies we have applied a reputation system to a networking scenario in which

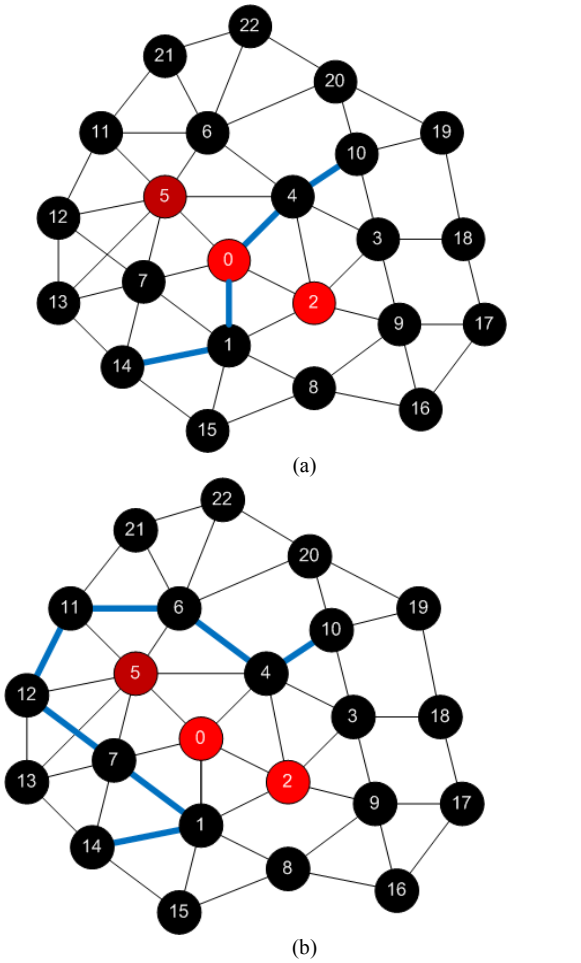


Fig. 2. An experimental result with the proposed reputation system (Source Node 14, Sink Node 10, Malicious Node 0 and Node 2 drop 25% routing packets, Malicious Node 5 drops 50% routing packets) (a) The shortest routing path without reputation system (b) The reliable routing path with the proposed reputation system (c) Accumulated packet drops throughout by simulation.

malicious relay nodes drop or manipulate packets. The reputation system employed the Bayesian update rule and cooperation between 2-hop neighbors. A routing algorithm was created to consider the reputation of the next-hop nodes during path selection. The simulations reveal that this fusion

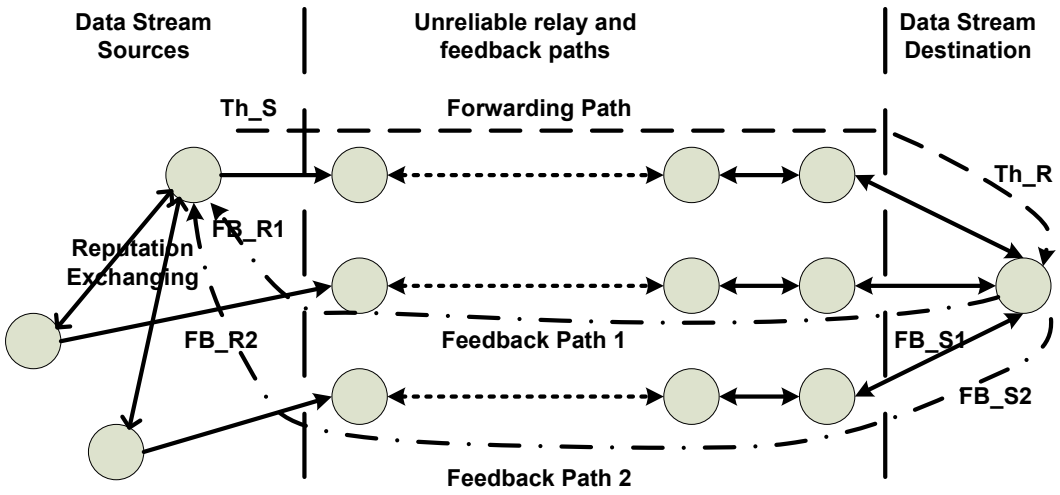


Fig. 3 Path reputation estimation with one forwarding path and multiple feedback paths

of a reputation system with a routing algorithm can find paths around malicious nodes (Figure 2).

III. Reputation combination and Path Reputation Estimation

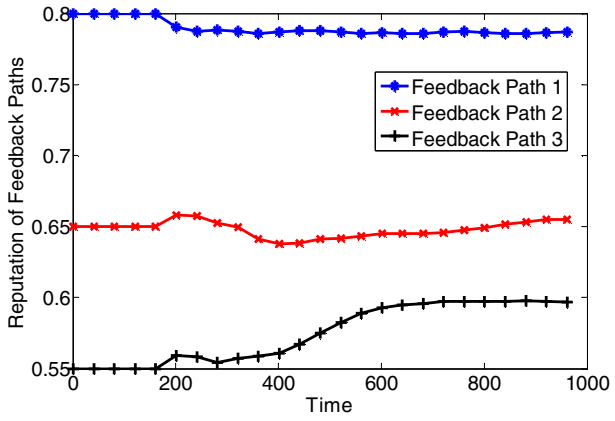
In a real system, one can usually collect multiple opinions towards a particular node from other nodes. Note that nodes which share their own opinions also have a reputation and sometime may distribute incorrect information due to many reasons, such as the node being compromised by an adversary. Effectively and properly combining these opinions will facilitate the establishing of a comprehensive reputation for the target. A Bayesian reputation computation based feedback combination system is discussed in this section by using a path reputation estimation example.

In an environment where multiple unreliable paths exist between the source and the destination, we can set up a collaboration scheme to estimate the reputation of the packet forwarding path with the help of feedback from the destination to the source transmitted along other paths. The reputation of the packet forwarding path here represents packet dropping and changing probability of a path. Note that feedback information is also delivered using unreliable paths, and packet dropping and situation changes can also take place. Thus delivering feedback information through multiple disjointed paths provides us redundant information and improves the accuracy of estimated reputation of the forwarding path. Furthermore, we can also estimate the reputation of a particular feedback path with redundant feedback information. The system diagram is shown in Fig. 3.

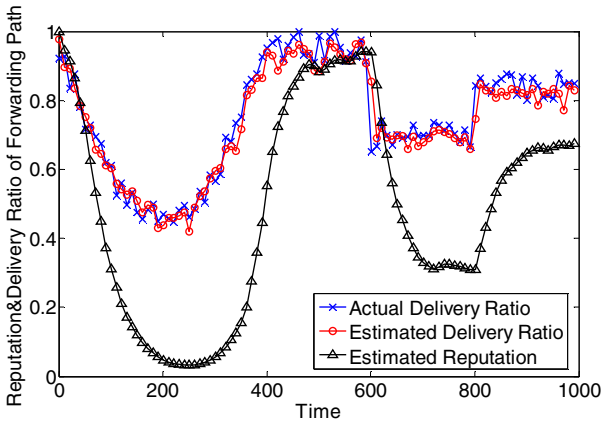
To alleviate overhead, the destination sends out feedback information at a much lower rate compared to data rate of the forwarding path. The feedback packet contains information reflecting the receiving throughput as well as the abstract information about the content with which the source can approximate the throughput and dropping/changing probability of the forwarding path. By assuming that most of the time the dropping/changing probability will not vary dramatically, the forwarding path dropping/changing probability is estimated through a weighted exponential average. The reputation of the forwarding path can be the same value of the dropping/changing probability, but if we are interested in a particular range, other functions, such as semi-Gaussian, can be used to enlarge the interested range and make values falling in that range more distinguishable. Fig. 4 shows the real time reputation estimation of a system with one forwarding path and three feedback paths. Fig. 4 (a) shows the reputation estimation of three feedback paths. The real time estimations are then feed into the reputation estimation of forwarding path shown in Fig. 4 (b). Here we use semi-Gaussian function to compute reputation since we are interested in the range of delivery ratio from 0.5 to 1. It is shown from Fig. 4 that the proposed reputation estimation system can track the dropping probability changes of forwarding paths precisely. Beginning with the proposed reputation estimation, forwarding path selection mechanism can be developed to ensure that maximum throughput from the source to the destination will be achieved dynamically.

IV. Cross-layer Design for Monitoring Security Context in Heterogeneous Networks

To realize desired security levels it will be critical to devise a cross-layered approach. Fig. 5 shows the proposed cross-layer design which considers the exchange of context from physical layer to application layer. A key advantage of a cross-layer design is that it allows protocols to become aware of the current network security state in an intra- and inter-node fashion. Our OPNET simulations [10, 11]



(a)



(b)

Fig. 4 Reputation estimation of forwarding and feedback paths

demonstrated the performance gains of team reinforcement learning over current protocols in heterogeneous network environments (The performance gain was nearly 5 times higher throughput with 10 times lower control overhead over conventional OSPF and AODV).

V. A SIMULATION EXAMPLE OF REPUTATION SYSTEM FOR SITUATION-AWARENESS

True benefits of reputation system for situation-awareness may be in more realistic mission-critical wireless networks for a battle communication. Fig 6 shows the flow of events in a simulated reputation system for situation awareness in a battlefield wireless network. It is often hard to distinguish between intrusions and legitimate operations because of the dynamically changing topology and network environment. In such a dynamic situation, a military base may need to monitor the targets in a theatre of operations by deploying wireless relay nodes and sensor nodes. In the OPNET simulations, as shown in Fig 6 (c), we have tested the proposed reputation system for the reliable delivery of video streaming data from 20 wireless sensor nodes to a base through 3 wireless relay nodes (with 2 malfunctioned wireless relay nodes by malicious nodes). The total video traffic demand from sensor

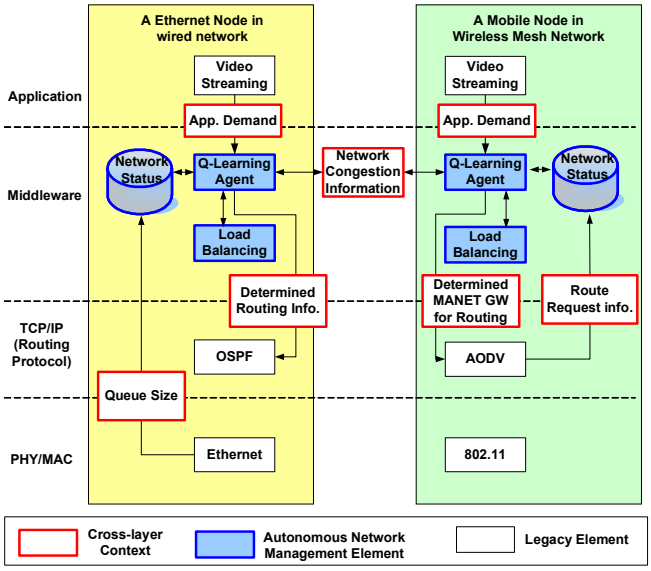
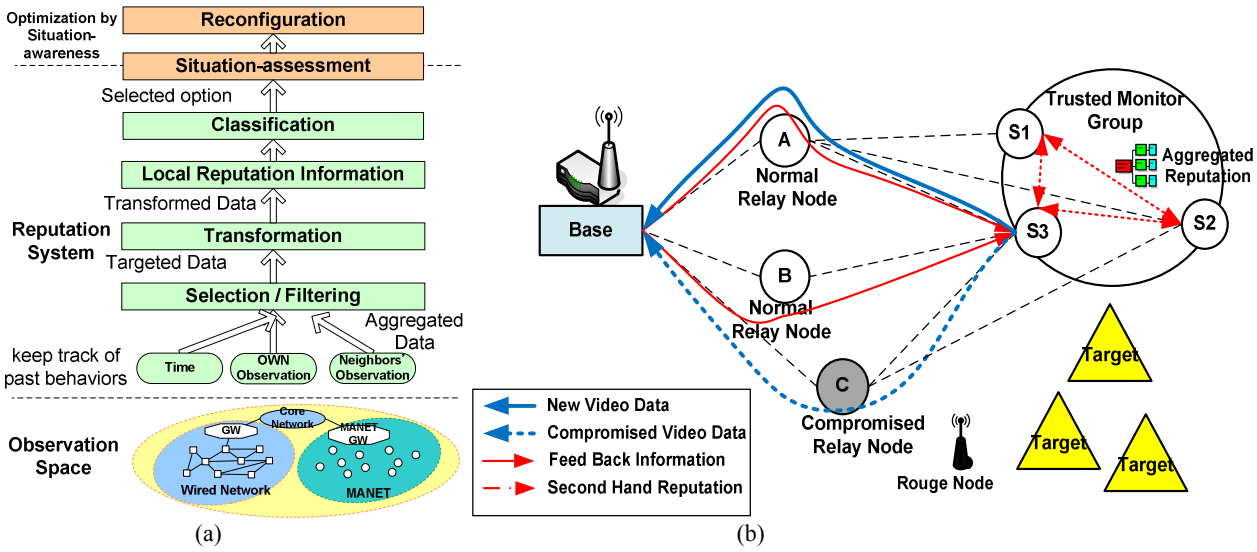


Fig. 5. Cross-layer design in OPNET for cognitive networking.

nodes to the base was 300Kbit/s. The wireless nodes were equipped with IEEE 802.11b wireless network interface and assumed to be random movement with a maximum speed of 10 m/s. The goal is reliable delivery of data to a group of nodes. However, the deployed nodes might drop the packets because they are misbehaving due to attack from adversaries (from simulation time t=180s). Baseline performance, measured in terms of AODV to facilitate wireless multi-hop routing, showed poor packet delivery ratio because sensor nodes were unaware of the malicious nodes and the malfunction of relay nodes (Relay_node_202 drop 33% routing packets Relay_Node_203 drops 50% routing packets). Fig. 6 (d) illustrates the successful packet delivery based on the proposed cooperative reputation system. By exploiting aggregated reputation information of relay nodes, reliable routing paths for consistent data streaming were formed resulting in nearly 4 times higher goodput during the attacks from malicious nodes (t>180s) : 267.66 KBit/s (7.23% Packet Loss Rate) vs. 82.29 KBit/s (57.90 % Packet Loss Rate).

VI. CONCLUSION

In this paper, we described a Computational Intelligence framework of cognitive security management for situation-awareness in heterogeneous networks. A reputation system has been proposed to improve the performance of routing protocols through the use of network state. We also presented some experimental results using OPNET. The performance results confirmed that by exploiting aggregated reputation information of relay nodes, reliable routing paths for consistent data streaming were formed resulting in nearly 4 times higher goodput during the attacks from malicious nodes.



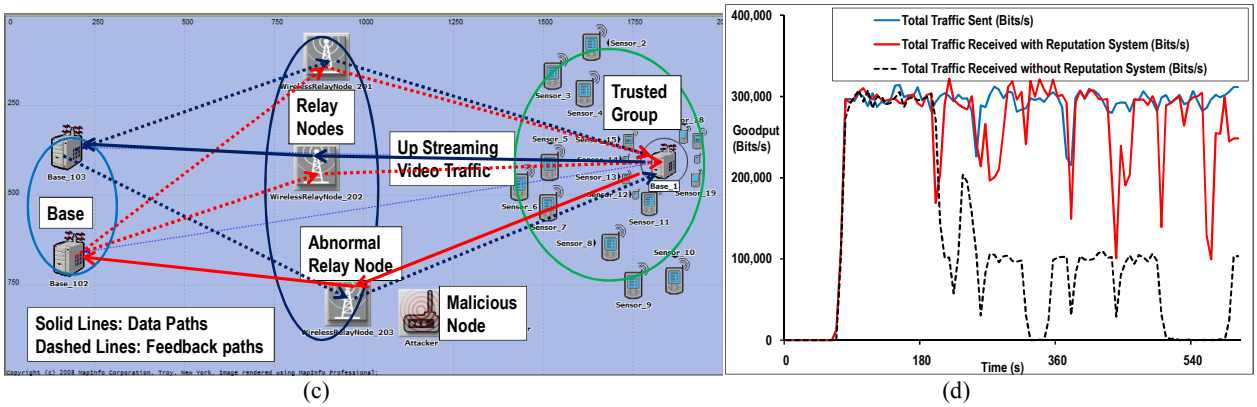


Fig. 6. The Reputation based Cooperation scheme (a) Overall Reputation System Flow for Situation-awareness (b) Building reliable routing paths by reputation system in a battlefield (c) OPNET simulation topology (d) Goodput with reputation system

REFERENCES

[1] R. Roman, J. Lopez, and S. Gritzalis, "Situation awareness mechanisms for wireless sensor networks," Communications Magazine, IEEE, vol. 46, pp. 102-107, 2008.

[2] D. Dasgupta and F. Nino, Immunological Computation: CRC Press, 2008.

[3] S. Sarafijanovic and J.-Y. L. Boudec, "An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks," Neural Networks, IEEE Transactions on, vol. 16, pp. 1076-1087, 2005.

[4] K. J. Mock and R. Vemuri, "Information filtering via hill climbing, WordNet and index patterns." vol. 33: Pergamon Press, Inc., 1997, pp. 633-644.

[5] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation systems." vol. 43: ACM, 2000, pp. 45-48.

[6] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile ad hoc networks by reputation systems," Communications Magazine, IEEE, vol. 43, pp. 101-107, 2005.

[7] M. Angermann, "Situation Awareness for Mobile Information Access in Heterogeneous Wireless Networks," Universität Ulm, 2004, p. 173.

[8] L. Santhanam, X. Bin, and D. Agrawal, "Selfishness in mesh networks: wired multihop MANETs," Wireless Communications, IEEE, vol. 15, pp. 16-23, 2008.

[9] S. Buchegger and J.-Y. L. Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," in P2PEcon, Harvard University, Cambridge MA, U.S.A., 2004.

Management with Reinforcement Learning for Wireless Mesh Networks," Lecture Notes in Computer Science, vol. 4786, pp. 168-179, 2007.

[11]M. Lee, X. Ye, D. Marconett, S. Johnson, R. Vemuri, and S. J. B. Yoo, "Autonomous Network Management Using Cooperative Learning for Network-Wide Load Balancing in Heterogeneous Networks," in Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, 2008, pp. 1-5.