Cooperation in Ad Hoc Network Security Services: Classification and Survey

José Montero-Castillo and Esther Palomar

Department of Computer Science
University Carlos III
Madrid, Spain
Email: {jmcastil, epalomar}@inf.uc3m.es

***Abstract*—Since ad hoc networks are infrastructureless and self-organized, their nodes have to cooperate in order to provide a particular service such as privacy or node incentives. In this paper, we elaborate on the cooperation role and management within the cooperation-based security services available in the literature. Furthermore, we present a comprehensive classification of such services and discuss what type of cooperation is realized inside of them.**

***Keywords*-ad hoc networks; cooperation-based schemes; security services; classification; survey**

I. Introduction

A. Need for Node Cooperation

Ad hoc networks consist of a set of hosts, more frequently called nodes, whose main and more frequent characteristics are [1]:

- Self-organization: nodes coordinate themselves in order to achieve a common set of goals, which means that there is no specialised authority in charge of organizing and orchestrating the network.
- Mobility: nodes can join and leave the network at will and they can change their position over time. Consequently, ad hoc networks become highly dynamic, lacking of a fixed topology.
- Wireless: nodes can communicate with other nodes through wireless links. If a node wants to communicate with a node out of its transmission range (i.e., a non-neighbouring node), packet routing becomes essential.
- Resource constraints: nodes have limited power, CPU, memory, bandwidth, etc. These limitations incite nodes to be selfish, trying to share their own resources as little as possible and trying to use other nodes' resources as much as they can.

Due to the dynamic nature of ad hoc networks, relying on a fixed infrastructure (i.e., servers, routers, public key infrastructure, etc.) turns out impractical [2]; hence, node cooperation becomes necessary. For example, if a node wants to send a message to some distant (i.e., not directly connected) node, since no router participates in the network, the only way for the message to be delivered is by having a network's subset of nodes cooperating to forward the message towards the destination.

As shown in the previous example, node cooperation is essential in ad hoc networks. But not only routing requires cooperation. Indeed, this paper focuses on the node cooperation realized inside of security services such as privacy or node incentives.

B. Our Contributions

The main contributions of our work are:

- Service-based classification: we propose a comprehensive service-based classification of the most important ad hoc network security services which have been addressed (at least once) by a cooperation-based approach.
- Cooperation analysis: for each classified service, we analyse a vast number of existing protocols from a cooperation point of view and describe the type of node cooperation found, if any.

The rest of the paper is organised as follows. In Section II, we have identified and classified the most important ad hoc network security services whilst analysing the type of cooperation realized in each of them. Finally, Section III summarizes the main points presented throughout the paper and establishes some future research directions.

II. A Comprehensive Classification

A. Overview

Due to the special characteristics that ad hoc networks have, the services deployed on top of them should not be exactly the same as the ones currently used in traditional networks. Instead, conventional approaches are being adapted by cooperation-based models. In this work, we study and classify the main security schemes applied to ad hoc networks from a service perspective. Moreover, a cooperation-based analysis is performed for each classified service. The different types of cooperative behaviours are detailed at the end of each category and references to existing protocols using such behaviours are provided. Furthermore, in Fig. 1, the classification proposed is depicted.

ISBN: 978-1-61208-171-7

B. Traditional Security

Many protocols designed for ad hoc networks leave security issues aside in order to prevent wasting the limited power and CPU that nodes in ad hoc networks usually have.

The different security services provided in ad hoc networks can be classified according to the type of security offered. This section surveys the cooperation-based schemes proposed for the security services deployed on top of ad hoc networks.

1) Intrusion Detection: Several works have addressed the intrusion detection by forcing nodes to cooperate in monitoring the network, gathering audit data and analysing it by applying certain behaviour patterns and statistical formulas. This type of service is usually implemented on a cluster-based ad hoc architecture.

The main characteristics that this type of service has regarding node cooperation are:

- Collecting audit data: audit data is collected by monitoring the network, a process which can be simultaneously performed by every node in the network [3], [4], [5] or by random sets of nodes changing every certain period of time [6], [7], [8].
- Analysing audit data: audit data can be analysed locally by each node [4] or can be sent to some special node in charge of analysing it [3], [5], [6], [7], [8].
- Deciding about an intrusion: based on the analysis results, deciding whether some abnormal behaviour corresponds to an intrusion or not can be decided locally by each analyser node [6], [7], [8] or in consensus by different analyser nodes [3], [4], [5].

2) Privacy: Privacy protection is usually applied to the routing process, protecting the sensitive information of senders, receivers and/or forwarders. But it can also be layered on top of any other process like the authentication one.

Cooperation-based privacy models are generally characterized by:

- Privacy in the routing process: in order to ensure the privacy the routing process, all the nodes in a particular route (except usually the destination) forward routing requests and replies in an anonymous fashion. In order to do that, different cryptographic algorithms can be used, being hash chains [9], asymmetric encryption [10], [11], [12] and symmetric encryption [13] ones of the most commonly utilized. Note that the onion encryption scheme is sometimes used together with asymmetric or symmetric encryption algorithms [11], [12].
- Privacy in the authentication process: a node may need to sign a message so as to authenticate itself against another node. In order to protect the privacy of the authenticating node, protocols can apply blind signatures [14], ring signatures [15] and group signatures [16].

3) Confidentiality: Confidentiality services prevent nodes from disclosing messages not intended for them.

A great many confidentiality services provided in ad hoc networks are based on traditional cryptography (symmetric or asymmetric), which is non-cooperative. However, there exists a cooperative scheme used to provide confidentiality in ad hoc networks: threshold encryption [17], [18], [19].

4) Integrity and Non-repudiation: Most of the services providing integrity and non-repudiation in ad hoc networks are based on traditional digital signatures, which are non-cooperative. However, there exists a cooperative scheme used to provide integrity and non-repudiation in ad hoc networks: threshold signatures [20], [21], [22]. Apart from this scheme, there are others providing integrity in a cooperative fashion:

- In [23], when a node sends a packet to some other node, the packet is coupled with a report generated by one of the nodes in the route towards the destination. The contents of the report are not specified in the paper. The reporting node is randomly and secretly (using symmetric encryption) selected by the sender.
- In [24], each node is monitored by a set of neighbouring nodes which are in charge of preventing the forwarding of illegally modified packets.

5) Authentication: Authentication services allow nodes to prove to other nodes that they are who they claim to be. Notice that this type of service can be applied to admission control but it is not an admission control service itself.

Most of the authentication services provided in ad hoc networks are based on the traditional two-node certificate exchange. Although the exchange itself is not cooperative, many protocols generate their certificates in a cooperative manner using schemes like threshold cryptography [25], [26], [27]. Apart from the use of threshold cryptography in the certification process, other cooperative schemes exist so as to provide authentication in ad hoc networks:

- In byzantine fault tolerant authentication schemes [28], [29], when a node A needs to authenticate a node B, it requests its trusted group to verify B's public key K_B. Each trusted group node challenges B with a random nonce encrypted with K_B and B replies to each of them with a signed message containing the received nonce.
- In [30], each sensor in a WSN requests a set of randomly chosen peers to authenticate its data.

6) Availability: This type of service depends basically on two types of availability: data availability and node availability. The former can be guaranteed by means of data replication [31]. The latter can be achieved by using powerful devices (which is out of the scope of this paper) and by preventing nodes from getting away from their routing responsibilities (issue that will be discussed later on in Section II-C).

Several cooperation-based data replication schemes share the following characteristics:

- Electing data managers: some replication protocols relies on one or more nodes in charge of determining what must be replicated and where such replicas must be allocated [31], [32], [33]. The process of electing such nodes can be achieved by consensus [31], [32] or by some other approach [33].
- Distributing replicas: most replication protocols distribute replicas directly from one node (usually the data man-

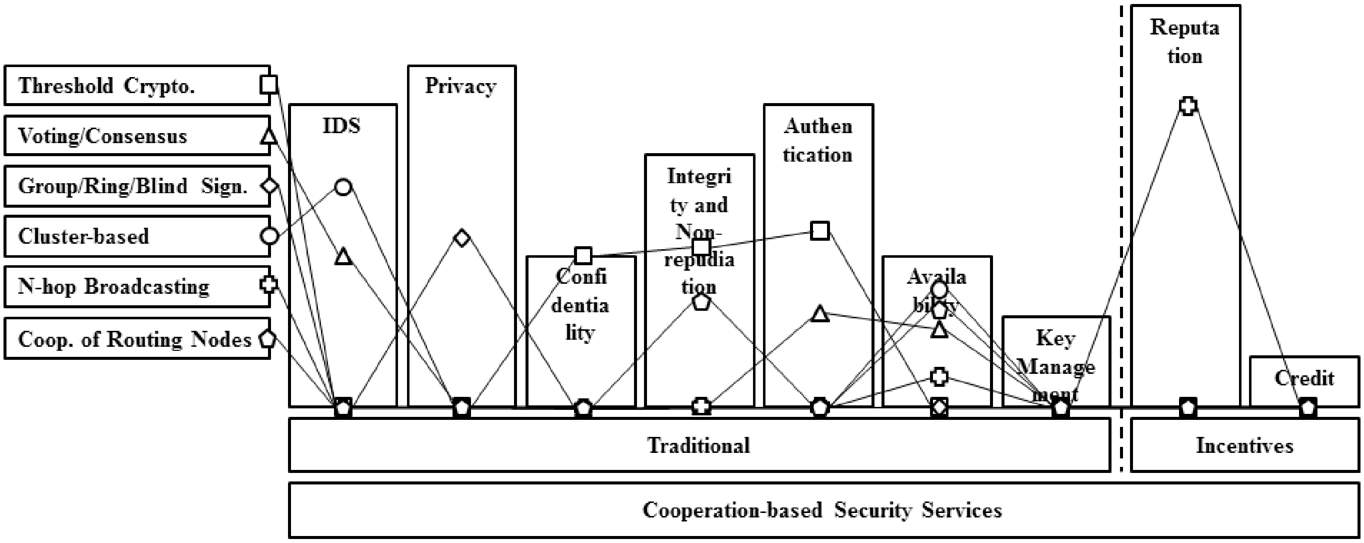

Fig. 1. Classification of cooperation-based ad hoc network security services. The height of the boxes representing services (e.g., IDS, privacy, etc.) roughly indicates the number of cooperation-based schemes which currently provide such service. The symbols (e.g., square, triangle, etc.) placed in the boxes are associated to types of cooperation (e.g., threshold cryptography, consensus, etc.) and the distance to the baseline roughly indicates the number of cooperation-based schemes which currently make use of such type of cooperation.

ager) to another (the replica holder) [31], [33], [34]; however, there exist protocols where the data to be replicated is broadcast in an N-hop area and the receivers replicate it if some particular conditions are fulfilled [32].

7) Key Management: Many of the security services described in the previous subsections rely on the use of cryptographic keys (symmetric or asymmetric). Now, we focus on the process of key generation, distribution, update and revocation.

Key distribution, update and revocation are not usually performed in a cooperative manner [26], [27], even though they can be fully decentralized. However, there exist cooperative schemes used to generate keys (symmetric and asymmetric):

- In [35], the private key of a network is cooperatively constructed: each node in a special set of nodes creates a partial key and shares it with the other nodes in the set. With all the partial keys, each node can construct the private key of the network.
- In [36], a symmetric key is cooperatively constructed using the multi-party version of the Diffie-Hellman protocol [37].

C. Incentives for Node Cooperation

Although the delivery of messages in an ad hoc network relies on the cooperation of its nodes, such cooperation does not always exist. Nodes may refuse to cooperate for many different reasons [38], [1]: reducing battery consumption, reducing memory usage, partitioning the network, performing a DoS attack, etc. Therefore, in order for ad hoc networks to properly function, nodes must be motivated to cooperate in forwarding messages.

In the literature, three main techniques are used to promote node cooperation [39], [40], namely trust models, reputation-based schemes and credit-based schemes. However, in this survey we are going to consider trust models as part of reputation-based schemes since both techniques end up using a numerical value to determine whether a node can be trusted or not.

1) Reputation-based Schemes: Reputation-based schemes determine if a node is trustworthy by considering its reputation. Generally, the reputation of a node is a numerical value defined as the perception that other nodes have, based on past observations, about its behaviour [41]. Reputation-based schemes can be further classified depending on whether they use indirect recommendations or not [39]. Schemes using direct recommendations rely only on local observations and therefore, nodes do not need to cooperate with other nodes in order to decide whether another node is trustworthy or not. Schemes using direct and indirect recommendations, however, rely not only on local observations but also on other nodes' observations; consequently, node cooperation is necessary.

Focusing on schemes using direct and indirect recommendations, we proceed to describe their main characteristics regarding node cooperation:

- Sharing reputation values: reputation values can be shared as indirect recommendations in a reactive and proactive manner. When a node asks other nodes for their reputation values (i.e., the reputation values they have regarding other nodes) [42], [43] in order to determine or update its own reputation values, the network is said to be sharing in a reactive fashion. When a node shares its reputation values periodically [44], [41], [45] or when a reputation value reaches a particular threshold [42], [46], [47], the network is said to be sharing in a proactive fashion.
- Selecting the sharing area: when a node shares its reputation values proactively, it can share them exclusively with neighbours [41], [44] or with any node in a N-hop

area [43], [47], [48] (note that the parameter N may be fixed for the whole network or variable depending on each node needs). On the other hand, when a node needs to communicate with its neighbours to share its reputation values, ask other nodes for their reputation values or forward the indirect recommendations received from a neighbour, it can communicate only with the neighbours it trusts [41], [48] or with all of them [42], [43], [44], [45], [46], [47].

- Selecting the range of values to share: nodes can be restricted to share only positive reputation values [49], only negative values [47], or both positive and negative values [41], [42], [44], [45], [46], [48]. So far, the most common choice is to allow nodes to share any reputation value.
- Assigning reputation values to new nodes: when a new node joins a network, its new neighbours must assign it a reputation value. Such value can be either a default one [41], [46], [47] or the result of asking other nodes for their reputation values [42], [45]. Using a default value forces the system to treat all new nodes in the same way. Asking other nodes for their reputation values allows the system to assign past-aware reputation values to new nodes. Obviously, for this latter technique to be useful, it is necessary that a new node can be identified as having participated in the network in the past.

2) Credit-based Schemes: Credit-based schemes try to prevent nodes from dropping packets by considering the forwarding process as a chargeable service: nodes forwarding packets receive micro-payments, and in return, they can use such micro-payments to send their own packets [50]. Credit-based schemes can be further classified as using tamper-proof hardware or using virtual bankers [39], [51]. *Schemes using tamper-proof hardware* ensure that each node will apply the payment scheme properly by executing all the logic inside a tamper-proof module. This means that a node does not need to cooperate with other nodes in order to know if another node has enough credit to pay its services. *Schemes using virtual bankers* rely on one or several nodes in charge of keeping track of each node's credit and ensuring that only nodes with enough credit can send packets. Most of these schemes use trusted third parties as virtual bankers and thus, nodes do not need to cooperate with other nodes in order to determine if a particular node can afford sending a packet. Nevertheless, there exist a few schemes using virtual bankers where nodes do cooperate in the payment process:

- In [52], the network is divided in cliques (i.e., groups) and each clique has a set of delegation nodes (one per wireless link) and a master. Periodically, the delegation nodes collect, compute and send to the master node information about flow rates. The master uses this information to calculate a list of prices and then, sends it to all the delegation nodes in its clique.
- In [53], each node broadcasts the set of price coefficients that it will use to charge other nodes. Although the paper does not specify how the payment is actually performed, it is obvious that some virtual banker must exist to ensure that the broadcast prices are correct.

III. Conclusion & Future Work

This paper focused on cooperative ad hoc network security services. We proposed a comprehensive service-based classification of the most important ad hoc network security services which have been addressed (at least once) by a cooperation-based approach.

Our analysis shows that node cooperation is not widely deployed in all types of ad hoc network services, in spite of the fact that node cooperation can provide services with a high level of robustness, fault-tolerance and completeness. For this reason, we are currently studying the possibility of including node cooperation inside ad hoc anonymous authentication services.

References

[1] D. Djenouri, L. Khelladi, and A. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[2] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[3] H. Li and D. Gu, "A novel intrusion detection scheme using support vector machine fuzzy network for mobile ad hoc networks," in *2nd Pacific-Asia Conference on Web Mining and Web-based Application*, 2009, pp. 47–50.

[4] Y. Fu, J. He, and G. Li, "A distributed intrusion detection scheme for mobile ad hoc networks," *Annual International Computer Software and Applications Conference*, vol. 2, pp. 75–80, 2007.

[5] Y. Fu, J. He, L. Luan, G. Li, and W. Rong, "A key management scheme combined with intrusion detection for mobile ad hoc networks," in *Agent and Multi-Agent Systems: Technologies and Applications*. Springer Berlin / Heidelberg, 2008, vol. 4953, pp. 584–593.

[6] Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. ACM, 2003, pp. 135–147.

[7] H. Deng, R. Xu, J. Li, F. Zhang, R. Levy, and W. Lee, "Agent-based cooperative anomaly detection for wireless ad hoc networks," *International Conference on Parallel and Distributed Systems*, vol. 1, pp. 613–620, 2006.

[8] K.-W. Yeom and J.-H. Park, "An immune system inspired approach of collaborative intrusion detection system using mobile agents in wireless ad hoc networks," in *Computational Intelligence and Security*. Springer Berlin / Heidelberg, 2005, vol. 3802, pp. 204–211.

[9] P. Xiong, W. Zhang, and F.-k. Shen, "A novel solution for protecting privacy in ad hoc network," in *Proceedings of the 2008 International Conference on Advanced Language Processing and Web Information Technology*. IEEE Computer Society, 2008, pp. 404–411.

[10] J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc networks," in *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, 2009, pp. 332–341.

[11] S. Taheri, S. Hartung, and D. Hogrefe, "Achieving receiver location privacy in mobile ad hoc networks," in *IEEE 2nd International Conference on Social Computing*, 2010, pp. 800–807.

[12] K. Jiejun, H. Xiaoyan, and M. Gerla, "An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 8, pp. 888–902, 2007.

[13] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, 2005, pp. 1940–1951.

[14] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, pp. 2803–2814, 2008.

[15] Z. Zhi and Y. K. Choong, "Anonymizing geographic ad hoc routing for preserving location privacy," in *Proceedings of the 3rd International Workshop on Mobile Distributed Computing*, vol. 6. IEEE Computer Society, 2005, pp. 646–651.

[16] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the 4th ACM international workshop on Vehicular ad hoc networks*. ACM, 2007, pp. 19–28.

[17] V. Daza, J. Herranz, P. Morillo, and C. Ràfols, "Ad-hoc threshold broadcast encryption with shorter ciphertexts," *Electronic Notes in Theoretical Computer Science*, vol. 192, pp. 3–15, 2008.

[18] Z. Chai, Z. Cao, and Y. Zhou, "Efficient id-based broadcast threshold decryption in ad hoc network," in *Proceedings of the 1st International Multi-Symposiums on Computer and Computational Sciences*, vol. 2. IEEE Computer Society, 2006, pp. 148–154.

[19] K. Kaskaloglu, K. Kaya, and A. Selcuk, "Threshold broadcast encryption with reduced complexity," in *22nd international symposium on computer and information sciences*, 2007, pp. 1–4.

[20] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," in *IEEE Military Communications Conference*, 2007, pp. 1–7.

[21] R. Di Pietro, L. V. Mancini, and G. Zanin, "Efficient and adaptive threshold signatures for ad hoc networks," *Electronic Notes in Theoretical Computer Science*, vol. 171, pp. 93–105, 2007.

[22] R. Gennaro, S. Halevi, H. Krawczyk, and T. Rabin, "Threshold rsa for dynamic and ad-hoc groups," in *Advances in Cryptology EUROCRYPT 2008*. Springer Berlin / Heidelberg, 2008, vol. 4965, pp. 88–107.

[23] H. Choi, W. Enck, J. Shin, P. D. Mcdaniel, and T. F. Porta, "Asr: anonymous and secure reporting of traffic forwarding activity in mobile ad hoc networks," *Wireless Networks*, vol. 15, pp. 525–539, 2009.

[24] S. Ozdemir and H. Cam, "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, pp. 736–749, 2010.

[25] J. Luo, J.-P. Hubaux, and P. Eugster, "Dictate: Distributed certification authority with probabilistic freshness for ad hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 4, pp. 311–323, 2005.

[26] C. Ma and R. Cheng, "Information security and cryptology." Springer-Verlag, 2008, ch. Key Management Based on Hierarchical Secret Sharing in Ad-Hoc Networks, pp. 182–191.

[27] B. Wu, J. Wu, and E. B. Fern, "Secure and efficient key management in mobile ad hoc networks," in *Proceedings of 19th IEEE International Parallel & Distributed Processing Symposium*. IEEE Computer Society, 2005.

[28] V. Pathak and L. Iftode, "Byzantine fault tolerant public key authentication in peer-to-peer systems," *Computer Networks*, vol. 50, pp. 579–596, 2006.

[29] R. Chen, W. Guo, L. Tang, J. Hu, and Z. Chen, "Scalable byzantine fault tolerant public key authentication for peer-to-peer networks," in *Euro-Par 2008 Parallel Processing*. Springer Berlin / Heidelberg, 2008, vol. 5168, pp. 601–610.

[30] R. Di Pietro, C. Soriente, A. Spognardi, and G. Tsudik, "Collaborative authentication in unattended wsns," in *Proceedings of the 2nd ACM conference on Wireless network security*. ACM, 2009, pp. 237–244.

[31] T. Hara and S. K. Madria, "Data replication for improving data accessibility in ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 5, pp. 1515–1532, 2006.

[32] P. Bellavista, A. Corradi, and E. Magistretti, "Redman: a decentralized middleware solution for cooperative replication in dense manets," in *3rd IEEE International Conference on Pervasive Computing and Communications Workshops*, 2005, pp. 158–162.

[33] H. Yu, P. Martin, and H. Hassanein, "Cluster-based replication for large-scale mobile ad-hoc networks," in *International Conference on Wireless Networks, Communications and Mobile Computing*, vol. 1, 2005, pp. 552–557.

[34] S. Lim, W.-C. Lee, G. Cao, and C. R. Das, "A novel caching scheme for improving internet-based mobile ad hoc networks performance," *Ad Hoc Networks*, vol. 4, pp. 225–239, 2006.

[35] A. Gupta, A. Mukherjee, B. Xie, and D. P. Agrawal, "Decentralized key generation scheme for cellular-based heterogeneous wireless ad hoc networks," *Journal of Parallel and Distributed Computing*, vol. 67, no. 9, pp. 981–991, 2007.

[36] N. Asokan and P. Ginzboorg, "Key agreement in ad hoc networks," *Computer Communications*, vol. 23, no. 17, pp. 1627–1637, 2000.

[37] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the 3rd ACM conference on Computer and communications security*. ACM, 1996, pp. 31–37.

[38] Z. Li and H. Shen, "Analysis of a hybrid reputation management system for mobile ad hoc networks," in *Proceedings of the 18th Internatonal Conference on Computer Communications and Networks*, 2009, pp. 1–6.

[39] G. F. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for manets: a survey," *Wireless Communications and Mobile Computing*, vol. 6, no. 3, pp. 319–332, 2006.

[40] M. Mejia, N. P. a, J. L. Munoz, and O. Esparza, "A review of trust modeling in ad hoc networks," *Internet Research*, vol. 19, no. 1, pp. 88–104, 2009.

[41] J. Liu and V. Issarny, "Enhanced reputation mechanism for mobile ad hoc networks," in *Trust Management*. Springer Berlin / Heidelberg, 2004, vol. 2995, pp. 48–62.

[42] Y. Rebahi, V. Mujica, and D. Sisalem, "A reputation-based trust mechanism for ad hoc networks," *IEEE Symposium on Computers and Communications*, vol. 0, pp. 37–42, 2005.

[43] Y. L. Sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, 2006.

[44] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for mobile ad-hoc networks," IC/2003/50, EPFL-IC-LCA, Tech. Rep., 2003.

[45] Q. He, D. Wu, and P. Khosla, "Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks," in *IEEE Wireless Communications and Networking Conference*, vol. 2, 2004, pp. 825–830.

[46] C. S. Y. Rebahi, V. Mujica and D. Sisalem, "Safe: Securing packet forwarding in ad hoc networks," in *Proceedings of the 5th Workshop on Applications and Services in Wireless Networks*, 2005.

[47] S. JianHua and M. ChuanXiang, "A reputation-based scheme against malicious packet dropping for mobile ad hoc networks," in *IEEE International Conference on Intelligent Computing and Intelligent Systems*, vol. 3, 2009, pp. 113–117.

[48] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2002, pp. 226–236.

[49] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security*, 2001, pp. 107–121.

[50] P. Marbach and Y. Qiu, "Cooperation in wireless ad hoc networks: a market-based approach," *IEEE/ACM Transactions on Networking*, vol. 13, pp. 1325–1338, 2005.

[51] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *Computing Research Repository*, 2003.

[52] Y. Xue, B. Li, and K. Nahrstedt, "Optimal resource allocation in wireless ad hoc networks: A price-based approach," *IEEE Transactions on Mobile Computing*, vol. 5, pp. 347–364, 2006.

[53] C. Tan, M. Sim, and T. Chuah, "Fair power control for wireless ad hoc networks using game theory with pricing scheme," *IET Communications*, vol. 4, no. 3, pp. 322–333, 2010.