A Candour-based Trust and Reputation Management System for Mobile Ad Hoc Networks

Eric Chiejina, Hannan Xiao and Bruce Christianson

School of Computer Science,University of Hertfordshire,Hatfield, Herts, UK

Email:{e.chiejina, h.xiao, b.christianson}@herts.ac.uk

Abstract. The decentralized administrative controlled-nature of mobile ad hoc networks (MANETs) presents security vulnerabilities which can lead to attacks such as malicious modification of packets. To enhance security in MANETs, Trust and Reputation Management systems (TRM) have been developed to serve as measures in mitigating threats arising from unusual behaviours of nodes. In this paper we propose a candour-based trust and reputation system which measures and models reputation and trust propagation in MANETs. In the proposed model Dirichlet Probability Distribution is employed in modelling the individual reputation of nodes and the trust of each node is computed based on the node's actual network performance and the quality of the recommendations it gives about other nodes. Cooperative nodes in our model will be rewarded for expanding their energy in forwarding packets for other nodes or for disseminating genuine recommendations. Uncooperative nodes are isolated and denied the available network resources. We employed the Ruffle algorithm which will ensure that cooperative nodes are allowed to activate sleep mode when their service is not required in forwarding packets for its neighbouring trustworthy nodes. The proposed TRM system enshrines fairness in its mode of operation as well as creating an enabling environment free from bias. It will also ensure a connected and capacity preserving network of trustworthy nodes.

1 Introduction

Unstructured networks are networks with a decentralized control of operations. Such networks lack centralized infrastructure and administration. Mobile ad hoc networks (MANETs) are unique examples of unstructured networks. MANETs are characterized by limited bandwidth and are less efficient unlike wireless networks with a centralized administration. Typically, a MANET is prone to eavesdropping, high security threats, rapid and continuous changes in network topologies due to nodes mobility [1]. Due to these distinguished features, all network nodes in a MANET must act as a router, server and client [2], mandating these nodes to collaborate for the effective and efficient operations of the network. Specialised network protocols have been employed in network layer of nodes in MANETs to ensure cooperation among nodes. Moreover, it is usually assumed that all the network nodes will act in accordance to the application and protocol specifications. However, due to limited resources or anomalous behaviours of some nodes, these assumptions are not always true. Network nodes sometimes make local decisions on whether to follow the network basic operations or not. These nodes may decide to act either selfishly by not forwarding packets or maliciously by advertising false routes [3]. Such an abrupt change in a node's behaviour may result in reduced network efficiency and

increased susceptibility to attacks. Therefore, a trust management system that ensures an effective and reliable collaboration of all network nodes in a MANET is essential. These systems would ensure that network nodes build a good reputation and attain a certain level of trust before such nodes can effectively operate in a network. As a result, there would be a significant reduction or elimination of malicious nodes trying to disrupt the operations of the network. Therefore, this would ensure that legitimate network nodes attain the required goals [3]. The rest of the paper is organised as follows: Section 2 introduces literature about trust and reputation systems in MANETs. In section 3, the concept of the proposed candour-based system is explained. Section 4 concludes the benefits of the proposed system and outlines future work.

2 Literature Survey

Over the past decade, a lot of research works have been proposed and carried out on TRM systems in mobile ad hoc networks which employed Price-based and Reputation-based schemes to enforce cooperation among nodes in the network. The Price-based schemes [4-9] treat packet forwarding as a service which can be paid for and they introduce a form virtual currency to regulate packet-forwarding collaboration among nodes. Most of the price-based schemes require tamperproof hardware [4], [5] or virtual banks that all the nodes in the network can trust [6], [7]. These price-based schemes use the virtual currency as a form of reward to nodes that participate in packet forwarding activities. In the case where a trust authority or virtual bank is required, it requires assistance from a fixed communication infrastructure to implement the reward schemes, which is not applicable for a pure ad hoc network.

On the other hand reputation-based schemes [10-23] employ different monitoring techniques in gathering data which are used in computing the reputation and trust of nodes in the networks. The monitored data can be derived from direct observations of nodes activities or from recommendations from other nodes. These reputation-based systems are geared towards punishing and isolating selfish or malicious nodes in the network by denying these uncooperative nodes the available network resources. The cooperative nodes are allowed to carry on with their normal network activities which are perceived as a reward by these systems as long as they continue to forward packets for other nodes. For example, He at al [15] proposed a secure and objective reputation-based incentive scheme for MANETs. The reputation of nodes in their proposed model is quantified by objective measures, and the propagation of reputation is efficiently secured by one-way-hash-chain based authentication. Their model uses punishment as a way of encouraging packet forwarding and discipline selfish nodes by probabilistically dropping packets that originates from those nodes.

Most of the existing reputation-based schemes suffer from lack of effective mechanisms to measure and propagate reputation and trust in the network. Secondly, the cooperative nodes in these reputation-based schemes are not truly rewarded for continuously expending energy in routing or forwarding packets. The continuous unrewarded cooperation results in low energy levels in these cooperative nodes. This may in turn have an adverse effect on their trust, reputation as well as individual network performance. As a

result, such nodes may end up being punished and isolated from the network when attempting to route or forward packets again. Therefore there is need for a reliable trust and reputation management system that would enforce cooperation by ensuring that collaborative nodes are rewarded for conducting favourable network operations, while selfish and malicious nodes are punished and isolated from the network. Hence, a Trust and Reputation Management system that incorporates punitive and incentive measures in its mechanism will ensure a fair platform for all the nodes in the network. In this paper we proposed a candour-based trust and reputation management system. This candour-based TRM system enshrines fairness in its mode of operation. Furthermore, it creates an unbiased enabling environment, which ensures that nodes are rewarded, isolated or punished based on the individual network behaviours of the nodes. Nodes in the proposed system are given incentive for expending their energy in forwarding packets for other nodes and for disseminating genuine second-hand reports. Our proposed TRM system considers that nodes have limited energy. Its functions cater for situations that will hamper an active nodes performance level due to low energy. It considers the fact that genuine nodes which are unable to forward packets due to low energy may still provide accurate recommendations. These recommendations usually require low amount of energy to action.

3 The Candour-Based TRM System

Fig. 1 shows the overview of the proposed candour-based TRM system. The following subsections explain the various module of the system.

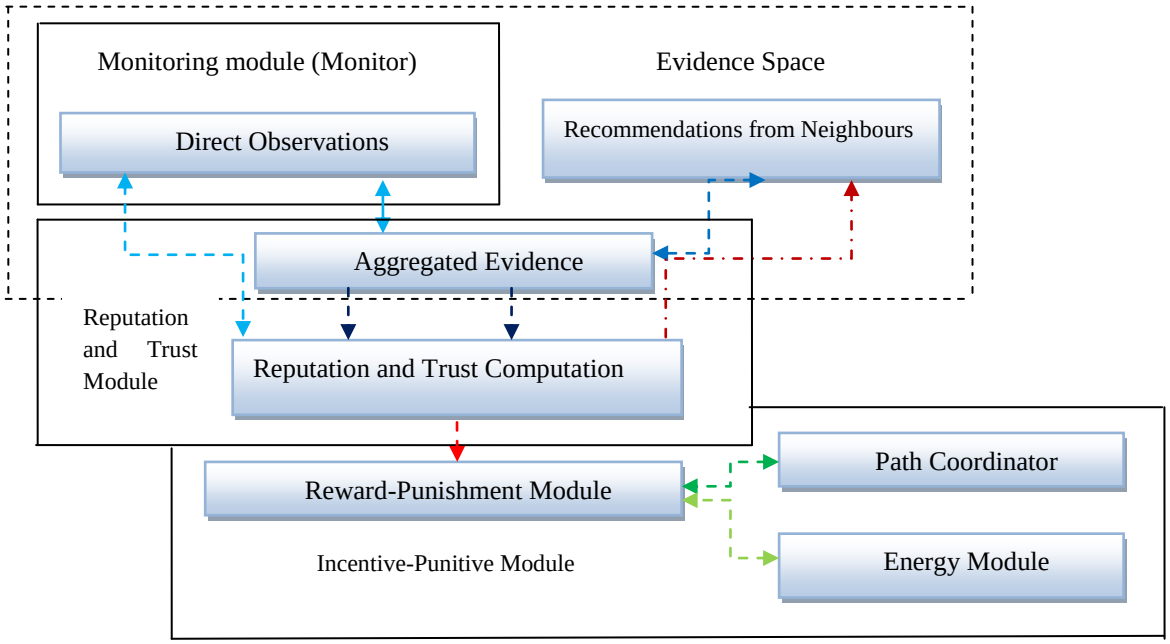

Fig. 1. The schematic diagram of the candour-based TRM system

3.1 The Monitor Module

The monitoring module comprises entirely of the monitor which is an essential part of the proposed TRM system. It specializes in detecting and reporting successful and unsuccessful packet forwarding activities and malicious modification of packets. It also ensures that nodes are not unfairly penalized for unintentionally dropping packets whereas the actual cause may be due to packet collision. To ensure the viability of the proposed monitoring process that will be carried out by the monitor, the monitor will only observe the activities of nodes that are 1-hop away, and each node will have the ability to carry out Omni-directional transmission. The monitor incorporates the packet acknowledgements and packet precision techniques in its mode of operations. It captures packets through listening of transmissions in promiscuous mode. Through monitoring of passive acknowledgements and the packet precision method, a node will be able to determine if its next hop neighbour is exhibiting any of the following behaviours;

i. Carrying out a packet modification attack if the data contents have been dishonestly modified
ii. Effectuating latency delays by retarding the retransmission of packets
iii. Displaying a selfish behaviour by not forwarding a packet
iv. Carrying out a prevarication attack if a self-induced fallacious packet is transmitted
v. Acting like a black hole if the packet intended for forwarding is not retransmitted or dumped.
vi. Launching an impersonation attack if the IP addresses or the MAC addresses have been spoofed.

Fig. 2. The Internal structure of the Monitor

The monitor detects, investigates and registers abnormal behaviours of nodes and passes the direct observations and recommendations to the reputation and trust modules for evaluation and computation. The next section will explain how this will be carried out.

3.2 Reputation Computation

Nodes continuously observe the behaviours of their neighbours that are 1-hop away and compute a reputation value for the successful observations carried out. The reputation of nodes in the network is computed using the Dirichlet Probability Distribu-

tion. The Dirichlet Probability Distribution was chosen over other distributions because it provides a sound and flexible platform suitable for designing a practical reputation system [24]. Dirichlet Distribution is able to differentiate a very large amount of negative reports from large positive reports. It is also useful in implementing reputation reports with grade levels, i.e. very bad – bad – uncertain – good – very good. This will enable nodes in the proposed TRM system to evaluate and decides which recommendation to integrate in computing the total aggregated reputation of a node in the network. The Dirichlet Probability Density Function (*PDF*) for a set of possible outcomes and for positive real parameters can be defined as [24, 25]:

$$f(\tilde{p} \mid \tilde{\alpha}) = \frac{\Gamma[\sum_{i=1}^{k} \alpha_i]}{\prod_{i=1}^{k} \Gamma[\alpha_i]} \prod_{i=1}^{k} p(\theta_i)^{\alpha_i - 1} \quad (1)$$

Where $\tilde{p}$ represents the set of possible outcomes given by

$$\tilde{p} = \{p(\theta_i) | 1 \leq i \leq 3\} \quad (2)$$

such that $p(\theta_1)$ may represents the probability of forwarding packets, and $p(\theta_2)$ may represents the probability of dropped packets and $p(\theta_3)$ may represents the probability of maliciously modified packets.
$\tilde{\alpha}$ represents a set of positive real parameters such that

$$\tilde{\alpha} = \{ \alpha_i | 1 \leq \ i \ \leq 3 \} \quad (3)$$

The parameter α_i can be interpreted as the prior observation counts of the possible outcomes such that α_1 may represents the number of successfully observed packet forwarding, α_2 may represents the number of successfully observed packet dropping and α_3 may represents the number of successfully observed malicious modification of packets.

The reputation of a node in the network $\Re$, can be determined by the probability expectation of the Dirichlet Distribution given by the equation below [24, 25]:

$$\Re = \mathcal{E}(p(\theta_i) | z_i, q_k) = \frac{z_i + Cq_k}{C + \sum_{i=1}^{k} z_i} \quad (4)$$

$$\alpha_i = Cq_k + z_i \quad (5)$$

α_i can be interpreted as prior observation counts for the possible outcomes of the observed events out of a *k* possible events. *C* is the cardinality of the state space over which a uniform distribution is assumed. $z_i = (z_1 \ldots\ldots\ldots z_k)$ represents the accumulated evidence over the observed elements of the state space and q_k is the base rate parameter over the state space. In case where no evidence is available, the base rate alone determines the probability distribution of the events. (e.g. the case of new nodes in the network) [24, 25]. As more evidence becomes available as a result of

observations, the influence of the base rate diminishes; it reaches a point where the evidence alone determines the probability distribution of the events.

3.2.1 Evaluation of Recommendations from Neighbouring Nodes

Nodes rely on the recommendations from its neighbours in evaluating the total reputation value of a node. To avoid the effect of false second-hand reports affecting the reputation value, a deviation test will be carried out to determine the validity of the recommendation. The result of the deviation test will affect the reputation and trust value of the recommending node positively or negatively. This is similar to the work carried out in [17, 23]. For instance, if the reputation value of a node ***A*** on a subject node ***B*** is given as $\Re_1$ and the recommendations of node ***B*** from node ***C*** is given as $\Re_2$, the deviation test can be evaluated using difference in the expectation value of the Dirichlet Probability Distribution. Let ϑ be the deviation for the test;

$$\Longrightarrow |\{\mathcal{E}(p(\theta_i)|\, z_i, q_k)_{\,2}\} - \{\mathcal{E}(p(\theta_i)|\, z_i, q_k)_{\,1}\}| \geq \vartheta \tag{6}$$

Where $\mathcal{E}(p(\theta_i)|\, z_i, q_k)_1$ and $\mathcal{E}(p(\theta_i)|\, z_i, q_k)_2$ are the expectation values of $\Re_1$ and $\Re_2$ respectively. ϑ is always positive and acts as the threshold validating recommendations from other nodes.

3.2.2 Aggregating Direct Observations and Recommendations

To compute total reputation of node ***A*** about a subject node ***B*** after a certain period i.e. t + 1, the reputation derived from direct observations and the recommendations from other nodes are aggregated to give a final reputation value. This implies that the total aggregated reputation of node ***A*** about node ***B*** is given by;

$$\Re_{ab(t+1)} = \delta\, \Re_{ab(t)} + \varphi\, \vec{r}_{b(t+1)}\ , \quad 0 \leq \delta \leq 1 \tag{7}$$

Where $\vec{r}_{b(t+1)}$ is the sum of all the recommendations from node ***A*** 1-hop neighbours about node ***B*** during a given period t+1. $\Re_{ab(t)}$ is the current reputation value. δ is the decaying factor which controls the rate at which old reputation value decays after a given period, and it's such that $\delta \in [0, 1]$. φ is a small positive weight which acts as a discount factor. After n periods of time, the total aggregated reputation of node ***A*** about node ***B*** can be given as;

$$\Re_{ab(t+n)} = \delta^n\, \Re_{ab(t)} + \varphi\, \vec{r}_{b(t+n)}\ ,\ 0 \leq \delta \leq 1 \tag{8}$$

3.3 Trust Evaluation

The Trust evaluation of a node in the network is a combination of the aggregated reputation value and the accuracy of the node's recommendations about other nodes. It is denoted as $T\langle \Re, \omega \rangle$ which is a combination of two factors. $\Re$ denotes the trustworthiness of the node based on is the reputation as calculated in 8 which represents

the node's actual network operations, while ω will denote the trustworthiness based on the accuracy of the recommendations a node makes about other nodes.

3.3.1 Computation of Accurate Recommendations

The accuracy value of the recommendations made by a node denoted as χ, can be defined as follows

$$\chi \triangleq \frac{\eta}{\eta + \gamma}; \quad \text{for } 0 \leq \chi \leq 1 \tag{9}$$

Where η is the cumulative number of recommendations that are correct and γ is the cumulative number of recommendations that are incorrect. A value of χ = 1 indicates absolute accuracy, and a value of χ close to zero indicates low accuracy.
The confidence value, ϱ associated with the accuracy value χ is defined as [20];

$$\varrho = 1 - \sqrt{\frac{12\eta\gamma}{(\eta+\gamma)^2\,(\eta+\gamma+1)}}, \text{ where } 0 \leq \varrho \leq 1 \tag{10}$$

A value of ϱ close to 1 indicates high confidence in the preciseness of the computed accuracy value, while a value of ϱ close to 0 indicates low confidence in the computed accuracy value. The trustworthiness of a node based on the accuracy of its recommendations about other nodes can be given as a pair of the accuracy value, χ and the confidence value, ϱ, which is similar to the notion of trust evaluation of nodes based on packet forwarding activities applied in [19,20].
The trustworthiness evaluation associated with the pair (χ, ϱ) can be defined as;

$$\omega(\chi,\varrho) \triangleq 1 - \frac{\sqrt{\frac{(\chi-1)^2}{m^2} + \frac{(\varrho-1)^2}{n^2}}}{\sqrt{\frac{1}{m^2} + \frac{1}{n^2}}} \tag{11}$$

where m and n are parameters that determine the relative importance of the accuracy value and the confidence value.

3.3.2 Total Trustworthiness of a Node

The total trustworthiness of a node is computed by combining the trustworthiness based on the reputation of the node in terms of what it does .i.e. forwarding packets, and in terms of the accuracy of its recommendation as defined in equation (10).
This implies that the total trustworthiness, $\mathbf{T}\,\langle \Re, \omega(\chi,\varrho)\rangle$ can be given as;

$$\mathrm{T}\,\langle \Re, \omega(\chi,\varrho)\rangle \;=\; [\Re,\ \omega(\chi,\varrho)\,] \tag{12}$$

3.4 The Reward and Punishment Scheme

The reward and punishment scheme ensures that collaborating nodes are rewarded for effectively carrying out network operations, while selfish and malicious node will be denied network resources and isolated from the network. After the reputation and

trust of a node in the network has been computed, nodes that are found to have trust and reputation values below the given threshold value are classified to be untrustworthy, while the nodes that have trust and reputation values that are above the threshold value are classified as trustworthy nodes in terms of their actual network activities and in terms of their recommendations about other nodes. The computed trust and reputation values of nodes are stored in a trust table. These values are periodically updated when new values are computed from newly accumulated observations. The Path Coordinator is responsible for isolating and denying misbehaving (untrustworthy) nodes the available network resources. It accesses the trust table before making a routing decision to ensure that untrustworthy nodes are eliminated from the routing paths. It also ensures that any packets that originate from those untrustworthy nodes are rejected. This ensures that only paths with trustworthy nodes are used for routing or forwarding packets. On the other hand, the reward scheme ensures that nodes that are found trustworthy are able to activate an idle period. It works with the observation that when a region of the network has a sufficient density of trustworthy nodes, only a small number of the nodes needs to be on at any time to forward traffic for active connections. The reward scheme decision is based on an estimation of how many of its trusted neighbours will benefit from it being awake, and the amount of energy available to it. The scheme employs a Ruffle algorithm [26] which ensures minimum power assignment for each trustworthy node such that symmetric connectivity is preserved.

For instance given a region of trustworthy nodes T_n = (W,E,c) with maximum power assigned to each node. The Ruffle algorithm aims to find a minimum power assignment for each of the trustworthy nodes in the network such that the symmetric connectivity in T_n is preserved while packet forwarding and routing remains effective and efficient. The algorithm is as follows;

- *Assign to each of the trustworthy node an ID based on the energy level. This information is gotten from the energy module.*
- *The trustworthy nodes are then sorted by their ID.*
- *For each trustworthy node W_i(i = 1, n), find the number of connected trustworthy nodes in its neighbourhood. This information can be derived from the path coordinator.*
- *Find the distance to the closest trustworthy node that has an ID great than the ID of W_i for each connected trustworthy nodes to W_i.*
- *Find the distance S_d = distance of the furthest of all the closest trustworthy nodes.*
- *Reduce the range of W_i to S_d.*

The Ruffle algorithm also aims to reduce energy consumption on sending packets for trustworthy nodes which are wake up. With the successful implementation of the Ruffle algorithm, the reward scheme will ensure a connected and capacity preserving network of trustworthy nodes.

4 Conclusion and Future Work

This paper proposes a candour-based trust and reputation management system for mobile ad hoc network which will ensure that selfish and malicious nodes are eliminated and denied network resources while the trustworthy nodes are rewarded for forwarding packets. The proposed system will employ a reward scheme that allows trustworthy nodes to randomly activate idle time when their service is not required. This will preserve their energy and in turn prolong the life span of the network of trustworthy nodes. Future work comprises of the full implementation of the proposed model using C++ and NS 2.34, evaluating the effectiveness of the implemented model in detecting misbehaving nodes and rewarding trustworthy nodes.

REFERENCES

[1] J.H. Cho, A. Swami and I.R. Chen, "Mission-Dependent Trust Management in Heterogeneous Military Mobile Ad Hoc Networks," 15th International Command and Control Research and Technology Symposium, Santa Monica, California, June 2010.

[2] P. B. Velloso, R. P. Laufer, D. O. Cunha, O. Carlos, M. B. Duarte, and G. Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model", in Proc. IEEE Transaction on Network and Service Management, vol.7, no.7, September 2007.

[3] G. Theodorakopoulos and J. S. Baras. " Malicious Users in Unstructured Networks", In Proceedings of the IEEE International Conference on Computer Communications, A S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks" Anchorage, AK, USA, May 2007, p. 884 – 891

[4] L. Buttyan and J. Hubaux, "Enforcing service availability in mobile adhoc WANs," IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), Boston, MA, USA, August 2000.

[5] L.Buttyan and J. P. Hubaux, Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks? in Technical Report No. DSC/2001/046, August 2001.

[6] M. Jakobsson, J. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," Proceedings of Financial Crypto 2003, Gosier, Guadeloupe, January 2003.

[7] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, creditbased system for mobile ad-hoc networks," IEEE INFOCOM 2003, San Francisco, CA, USA, April 2003

[8] M. Felegyhazi, L. Buttyan, and J. Hubaux, "Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks - the static case", in Proc. Personal Wireless Communication (PWC), Venice, Italy, September 2003.

[9] J. Cai, U. Pooch, "Allocate fair payoff for cooperation in wireless ad hoc networks using Shapley Value", Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International , 26-30 April 2004

[10] S. Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehaviour in mobile ad hoc networks". In Proceedings of MOBICOM 2000, pages 255–265, 2000

[11] P. Michiardi and R. Molva, CORE: A COllaborative REputation mechanism to enforce node cooperation in mobile ad hoc networks, in Proc. 6th Int. Conf. Commun. Multimedia Security, 2002, pp. 107–121

[12] 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 , pp. 403-410, Canary Islands, Spain, January 2002.

[13] S. Bansal and M. Baker, “Observation-Based Cooperation Enforcement in Ad-Hoc Networks”, Technical Report, Computer Science Department, Stanford University, CA, July 2003.

[14] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, “Quantifying trust in mobile ad-hoc networks," in Proc. IEEE International Conf. Integration Knowledge Intensive Multi-Agent Syst., Waltham, USA, April 2005

[15] Q. He, D. Wu, and P. Khosla, “A secure incentive architecture for ad hoc networks," Wireless Commun. Mobile Comput., vol. 6, no. 3, pp. 333- 346, May 2006.

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

[17] S. Buchegger and J.-Y. L. Boudec, ”Performance analysis of the CONFIDANT Protocol”, in Proc. 3rd ACM Int. Symposium on Mobile Ad Hoc Network Computing, Lausanne, Switzerland, 2002, pp. 226–236

[18] J. Hu, “Cooperation in Mobile Ad Hoc Networks”, Technical report (TR-050111), Computer Science Department, Florida State University, Tallahassee. January 2005.

[19] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, “A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs,” in In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’05), pp. 1–10, November 2005

[20] C. 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 October 2006, pp. 23-34.

[21] A. A. Pirzada and C. McDonald, “Trust establishment in pure ad-hoc networks,” Wireless Personal Communications: An International Journal, vol. 37, no. 1-2, April 2006, pp. 139–168

[22] A. Boukerche and Y. Ren, “A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile AdHoc Networks,” Proc. Int’l Workshop on Modelling Analysis and Simulation of Wireless and Mobile Systems, Vancouver, British Columbia, Canada, pp. 88-95, 2008.

[23] S. Buchegger and J. Y. Le Boudec. "A Robust Reputation System for Mobile Ad-hoc Networks". In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2005.

[24] Josang, Audun; Haller, Jochen; "Dirichlet Reputation Systems," Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on, vol., no., pp.112-119, 10-13 April 2007

[25] Aboulwafa, S.; Bahgat, R.; "DiReCT: Dirichlet-based Reputation and Credential Trust management," Informatics and Systems (INFOS), 2010 The 7th International Conference on , vol., no., pp.1-8, 28-30 March 2010

[26] Brinza, D., Derado, G., Aznita, R., Li, Y. and Zelikovsky, A. (2004) `Energy efficient protocols for ad-hoc networks', Georgia Electronic Design Center Industry Advisory Board (GEDC IAB'04), ppt. Retrieved from http://cs.gsu.edu/~dima/dima/cv/index.html