Supplemental Material for "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing"

Ing-Ray Chen, Fenye Bao, MoonJeong Chang, and Jin-Hee Cho

APPENDIX A. RELATED WORK

DTNs have attracted much attention in the networking research community. Most DTNs are deployed in extreme environments (e.g., battlefields and developing regions), where the end-to-end connection which is the fundamental assumption of the Internet cannot be guaranteed [18]. Hence, protocols designed for the Internet may not be applicable to DTNs. Due to specific DTN characteristics and application requirements, [28] suggests a top-down approach for DTN-protocol design to consider application priorities. In this paper, we focus on trust management and secure routing in DTNs. We refer the readers to [18, 28] for research challenges in DTNs.

The literature is abundant in routing protocol design for DTNs. Traditional routing protocols [5, 7, 23, 32] for DTNs focus on exploring the mobility pattern and predicting future encounter events. However, in the presence of misbehaving nodes, these routing protocols still can experience a low message delivery ratio. A number of protocols have been proposed lately to cope with misbehaving nodes. *Detection* and *prevention* are two widely used approaches. Detection-based approaches [2-4, 16, 21, 24, 26, 27, 33] rely on trust/reputation techniques to identify misbehaving nodes and avoid selecting misbehaving nodes as message carriers in DTN routing. Prevention-based approaches assume that nodes are *rational* to maximize their own interests and often use incentives [8, 25, 30, 31, 34] to stimulate cooperation between nodes and avoid misbehavior. Well-behaved nodes are awarded while uncooperative nodes are punished such that a node would not misbehave for the sake of its own interest. However, incentive-based approaches in general will not work for malicious nodes with ultimate interests to disrupt the operation of the system. Also, the assumption of rational behavior following prescribed game strategies in general may not be justified in DTN environments. Context-free protocols [31] have also been proposed to hide the identity of the destination node in order to encourage selfish nodes to participate in packet forwarding. However, in intermittently connected DTN environments, message forwarding follows the store-carry-and-forward paradigm. It is difficult, if not impossible, to establish the entire routing path by the source node without revealing the identity of the destination node to intermediate carriers during DTN routing.

Unlike trust management for mobile ad hoc networks (MANETs) [13], trust management for DTNs is little explored in the literature. To the best of our knowledge, only [2, 3, 16, 21, 33] used feedback mechanisms or indirect recommendations for trust management. [33] considered three sources to estimate trust: cryptographic operation, node's behavior, and reputation. For cryptographic operations, encryption and decryption mechanisms are used to provide authentication and confidentiality and to defend outside attackers. A watchdog mechanism is adopted to detect node's behavior, and this information is combined with cryptographic operation using a weighted sum to generate a local trust value. Each node also exchanges its local trust evaluation as recommendation to others. A limitation of their work is that no consideration was given to inside attackers. [2, 3] designed an iterative trust management scheme for DTNs. They used discrepancies of indirect recommendations for adversary detection and used authentication as the underlying mechanism to evaluate a node. A node exchanges its trust evaluation with others and interactively updates its trust evaluation. Inconsistent trust evaluations are identified and removed iteratively until the trust evaluation converges. Not leveraging direct-observation based trust/reputation deriving from social networking is a main drawback of these approaches.

Compared to the works cited above, we also adjust feedback trust evaluation dynamically in response to changing network conditions. Moreover, our protocol takes direct evidence into consideration for trust aggregation. Bayesian trust management schemes [15, 17, 21] also combine direct and indirect observations to build trust values (by using a trust threshold). We will use a Bayesian trust management tailored for DTN routing as a baseline scheme for performance comparison in this paper. Very recently, [10, 11] considered both direct observations and indirect recommendations for trust management and applied it to encounter-based routing. However, only a theoretical analysis was given without validation. Different from [10, 11], our work is on *design* and *validation* of dynamic trust management for trust-based secure routing in DTNs.

In Table 1, we summarize existing trust management schemes for DTNs in the literature and compare them with

Table 1: A Comparison of Trust Management Schemes for DTNs.

Trust Management Scheme	Trust Model	Trust Protocol Design	Trust Metrics Considered	Direct / Indirect Trust	Trust Attacks Considered	Trust Protocol Validation	DTN Routing Performance Optimization
[2, 3]	Iterative Reputation	Trust aggregation	Delivery reception and feedback consistency	Both	Bad-mouthing, ballot-stuffing, and whitewashing	Based on mobility models	No
[10, 11]	Weighted Summation	Trust composition, trust aggregation, and trust formation	Honesty, cooperativeness, and connectivity	Both	Bad-mouthing, ballot-stuffing, and whitewashing	Based on random mobility models	No
[16]	Weighted Summation	Trust aggregation	Delivered and forwarded messages	Direct trust only	No	Based on mobility models	No
[15, 17, 21]	Bayesian Model	Trust aggregation	Positive feedback	Both	False recommendations	Based on mobility models	No
[33]	Weighted Summation	Trust aggregation	cryptographic operation, and node behavior	Both	No	Based on random mobility in a city area	No
Our proposed scheme	Weighted Summation	Trust composition, trust aggregation, and trust formation	Healthiness, unselfishness, energy, and connectivity	Both	Bad-mouthing, ballot-stuffing, and self-promoting	Based on both mobility models and real traces	Yes

our proposed scheme (the last entry in Table 1). We observe that our work expands the state of the art research in trust management for DTNs in both trust protocol design by considering trust composition, trust formation and application-level trust optimization issues in addition to trust aggregation, and trust protocol validation by considering both mobility models and real traces.

A number of papers have studied the effect of social relationships on the performance of DTN routing [6, 9, 14, 20, 22, 25]. These approaches aim to tolerate selfish behaviors in DTN routing, with no consideration given to malicious nodes, however. Game theoretical approaches have also been considered to stimulate cooperation of selfish nodes [8, 25]. However, if selfish nodes are not rational or do not follow game strategies, a low message delivery ratio would still result.

Compared to the works cited above, our protocol considers both social trust and QoS trust [13] in trust formation and does not make any assumption regarding rational behavior or game strategies taken by malicious/selfish nodes. Rather, our trust aggregation protocol relies on the use of direct trust evidence and indirect recommendations to aggregate trust proven to converge to ground truth.

In the area of mobility models for DTNs, it is concluded [9] that the popular random waypoint mobility model is inadequate to model the inter-contact time in human centric DTNs. Rather, the inter-contact time exhibits a heavy tail that can be lower bounded by the tail of a power law. Small Word in Motion (SWIM) [19] is a mobility model specifically designed to model social behavior among nodes based on human mobility. In this paper, we will test the validity of our protocol design with both SWIM and mobility traces.

APPENDIX B. SIMULATION VALIDATION

We validate analytical results through extensive simulation using ns-3 [1]. The simulated DTN environment is setup as described in Table 1 of [12]. We simulate two mobility patterns: a synthetic mobility model (SWIM) [19] and real mobility traces. We investigate four mobility traces from [29], namely *Intel*, *Cambridge*, *Infocom05* and *Infocom06*. Table 2 summarizes the experimental settings under which these mobility traces are obtained. During the experiment, each *internal device* records the contact/encounter event with other devices (*internal* or *external*). Due to the fact that the contact events between external devices are not recorded in the traces, we only consider internal devices in our simulation. We conduct sufficient simulation runs with disjoint random number streams and collect observations such that 5% accuracy and 95% confidence level requirements are satisfied. We mark the standard deviation from the mean by error bars in the data figures presented in this section.

Table 2: Experiment Settings for Mobility Traces.

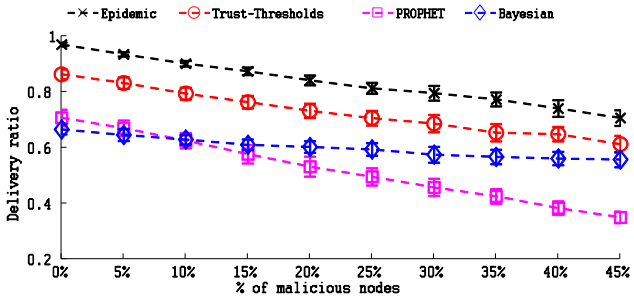
Trace	*Intel*	*Cambridge*	*Infocom05*	*Infocom06*
Participants	Researches & interns	Students & faculty	conference attendees	conference attendees
Experiment Time	4 days	5 days	3 days	4 days
Internal Devices	9 with 1 stationary	12	41	98 with 20 stationary
External Devices	119	211	233	4626

B.1 Simulation Results based on SWIM Mobility

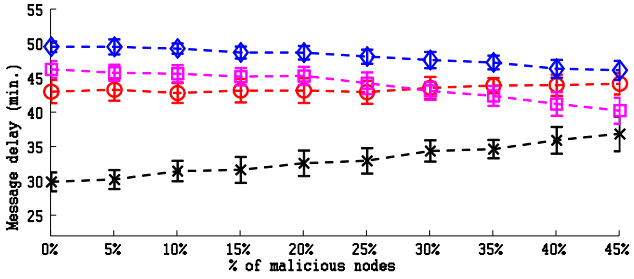
Figures 1(a), 1(b), and 1(c) show the simulation results in message delivery ratio, message delay, and message overhead of DTN routing under the SWIM mobility model, corresponding to the analytical results in Figures 5(a), 5(b), and 5(c) of [12]. We observe that the simulation results in Figures 1(a), 1(b), and to 1(c) are virtually identical to the analytical results. For all cases, the deviation of the simulation results from the analytical results is bounded by 3% MSE.

B.2 Simulation Results based on Mobility Traces

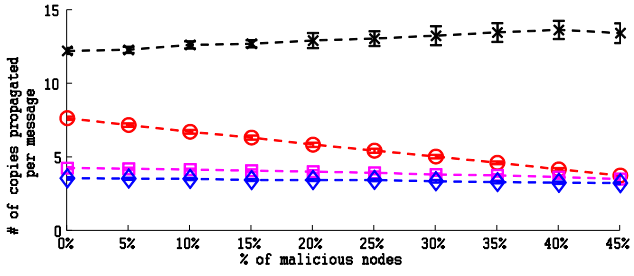
Figure 2 shows the simulation results of comparing our trust-based secure routing protocol against Bayesian trust-based routing, PROPHET, and epidemic routing protocols, based on *infocom06* mobility traces [29]. We choose *infocom06* over others since it consists of more nodes and lasts longer. The results of the other three mobility traces exhibit the same trend and thus are not shown here. Briefly,



(a) Delivery Ratio.

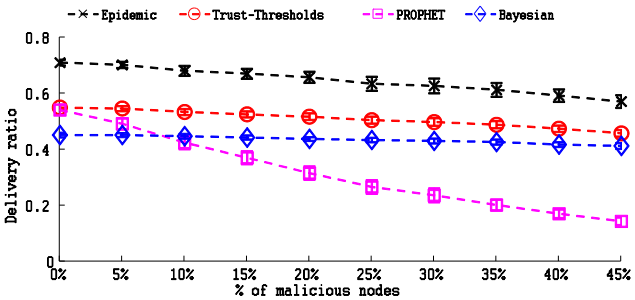


(b) Message Delay.

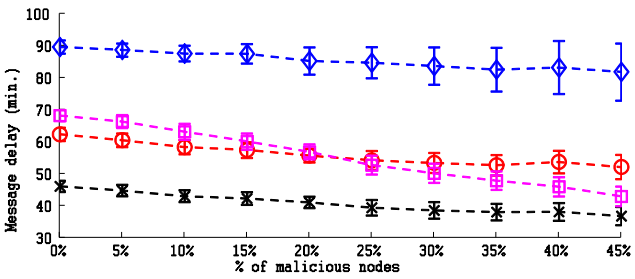


(c) Message Overhead.

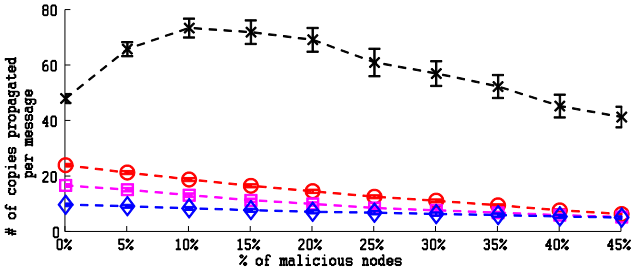
Figure 1: Simulation Results Corresponding to Analytical Results in Figure 5 of [12] based on SWIM Mobility.



(a) Delivery Ratio.



(b) Message Delay.



(c) Message Overhead.

Figure 2: Performance Comparison of Routing Protocols based on Mobility Traces.

the *infocom06* trace data contain encounter events collected by Bluetooth devices carried by conference attendees. There were a total of 98 Bluetooth devices (20 stationary nodes) used to record the encounter events over a period of four days. We select 78 mobile nodes in our simulation and use the encounter events in the traces as the time instances to perform trust updating and message forwarding (executed by each node). In each simulation run, we randomly pick a number of nodes as selfish nodes (30%) and malicious nodes (from 0% to 45%) and generate a social friendship matrix [22]. A malicious node performs attacks to disrupt the trust of the DTN, including self-promoting, ballot stuffing and bad-mouthing attacks. An altruistic node always forwards messages. A selfish node forwards a message only when it is a friend of the source, current carrier, or destination.

We first observe that Figures 2(a), 2(b), and 1(c) obtained based on mobility traces exhibit virtually the same trends as Figures 1(a), 1(b), and 1(c) obtained based on the SWIM mobility model. This supports our claim that our trust-based secure routing protocol can significantly outperform Bayesian trust-based routing and PROPHET in message delivery ratio regardless of the node encountering pattern. We further observe that Figure 2 (displaying simulation results based on traces) exhibits remarkably similar trends as Figure 5 in [12] (displaying analytical results based on SWIM movements) in terms of ranking routing protocols in delivery ratio, delay and overhead. As both simulation results based on traces (Figure 2) and SWIM movements (Figure 1) correlate well with analytical results (Figure 5 of [12]), we conclude that the analytical results obtained, along with the conclusions drawn, are valid.

B.3 Protocol Convergence, Accuracy and Resiliency

In this section we present simulation results to demonstrate trust assessment accuracy, convergence and resiliency properties of our protocol. We use the healthiness trust property as an example, because unlike all others it has an additional false negative probability parameter (P_{fn}) due to the possibility of a compromised node performing random attacks with probability P_{rand} to evade detection. Again we set P_{error} = 5% for direct detection error probability due to environment noises and $P_{fn} = P_{error}P_{rand} + (1 - P_{error})(1 - P_{rand})$. Also we set the % of malicious nodes to 30% so as to manifest the effect of random attacks.

Figure 3 shows the healthiness trust of a randomly selected healthy node (node i) toward a randomly selected compromised node (node j), i.e., $T_{i,j}^{healthiness}(t)$, as a function of time t with the random attack probability P_{rand} of node j varying in [0, 1]. We first observe that $T_{i,j}^{healthiness}(t)$ eventually converges to a trust value. The warm-up time to build up trust depends on the mobility pattern and encounter frequency. Second, we observe that the trust value is close to P_{fn} after convergence. Specifically, $T_{i,j}^{healthiness}(t)$ is close to 0.95 for a malicious node exhibiting no evidence of attacks with $P_{rand} = 0$; it is close to 0.05 for a malicious node performing reckless attacks with $P_{rand} = 1$; and it is close to 0.68 for a malicious node performing attacks with $P_{rand} = 0.3$. This demonstrates that both trust convergence and accuracy properties are preserved by our protocol with the converged trust value reflecting ground truth status.

Figure 4 shows the effect of random attacks to DTN routing performance. As expected, we see that the delivery ratio under random attacks ($P_{rand} < 1$) is higher than that under reckless attacks ($P_{rand} = 1$) since reckless attackers will always drop messages. Nevertheless, we see that the delivery ratio remains manageable as P_{rand} goes from 0 to 1. This demonstrates the resiliency property of our rust based routing protocol against random attacks by malicious nodes.

APPENDIX C. DYNAMIC TRUST MANAGEMENT

We demonstrate the effectiveness of our dynamic trust management protocol in response to changing environment conditions. Without loss of generality, we consider hostility changes over time as modeled by the dashed line entities in the SPN model shown in Figure 2 of [12] with the transition rate of T_COMPRO being λ_c. Under our dynamic trust management protocol, the best protocol settings in terms of (β, λ_d), w^X, and (T_f, T_{rec}) identified in Section 6 of [12] are applied in response to dynamically changing network conditions to minimize trust bias and to maximize DTN routing performance. Specifically, at runtime, each node senses hostility changes using its trust evaluation results (trust properties in healthiness) toward other nodes in the DTN, and then, based on the detected % of misbehaving nodes, performs a simple table lookup (e.g., into Tables 2 and 3 of [12]) to determine and apply the best protocol settings in (β, λ_d), w^X, and (T_f, T_{rec}) to minimize trust bias and to maximize DTN routing performance. As demonstrated in Figure 3, the healthiness trust $T_{i,j}^{healthiness}(t)$ toward a compromised node will converge to P_{fn} so a node can use the fraction of "active" malicious nodes detected (i.e., those for which $T_{i,j}^{healthiness}(t)$ falls below $P_{error} + 0.5$) to perform a table lookup. Also trust convergence takes time, so a node must apply optimal protocol settings proactively.

Below we perform a comparative analysis of our dynamic trust management protocol for DTN routing against PROPHET, Bayesian trust-based routing, and epidemic routing, all operating under best protocol settings dynamically in response to hostility changes over time. We consider two mobility patterns: the SWIM mobility model [19] and the *infocom06* mobility trace [29]. Table 3 describes the simulation setup for each mobility pattern. Initially, there is no malicious node in the network. As time progresses, nodes become malicious with rate λ_c. The data reported is based on the average of 2000 messages. The last message is issued a few hours (the maximum delay) before the end of simulation to ensure sufficient time for message delivery.

Figure 5 shows performance comparison results based on the SWIM mobility model. We observe that our dynamic trust-based routing protocol performs comparably to epidemic routing protocol in delivery ratio, while the other two protocols (PROPHET and Bayesian trust-based routing) have a low delivery ratio. The reason is that our trust-based routing protocol operating under the best (β, λ_d) setting can accurately identify misbehaving nodes with minimum trust bias (through the healthiness and

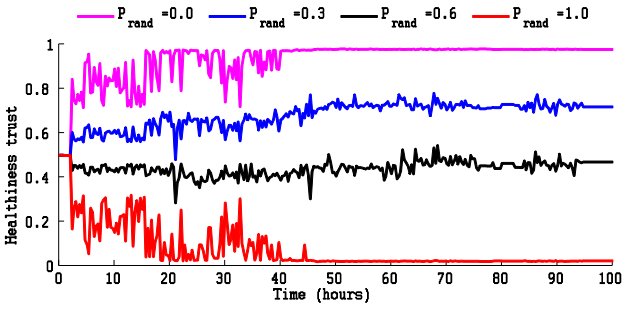


Figure 3: Healthiness Trust Evaluation under Random Attacks.

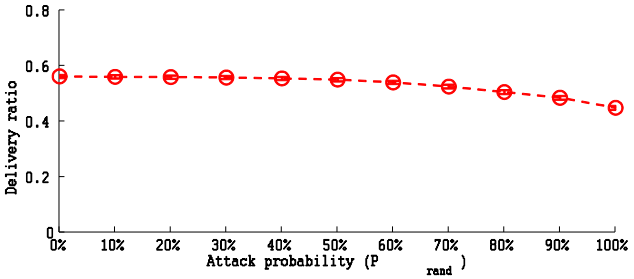
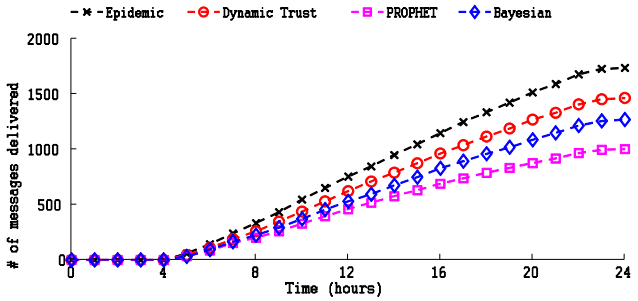


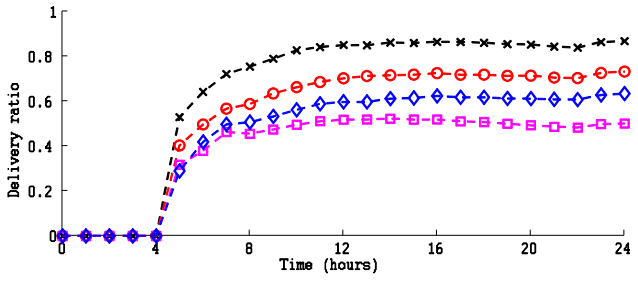
Figure 4: Message Delivery Ratio under Random Attacks.

Table 3: Dynamic DTN Environment Setup.

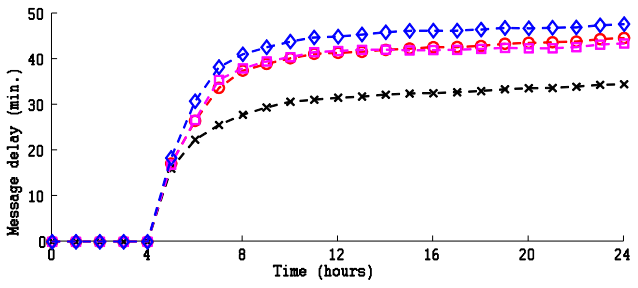
Mobility	***SWIM***	***Infocom06 Trace***
Simulation time	24 hours	100 hours
Compromise rate (λ_c)	0.03 / hour	0.0072 / hour
# of Messages per run	2000	2000
Warm-up time	4 hours	10 hours
Maximum delay	2 hours	5 hours
MAC & PHY	IEEE 802.11a, Ad-Hoc	
Energy model	3V, 17.4mA TX, 5.8mA RX, 0mA IDLE	



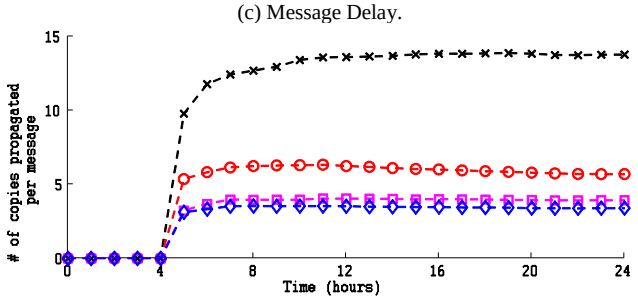
(a) Number of Delivered Messages.



(b) Delivery Ratio.

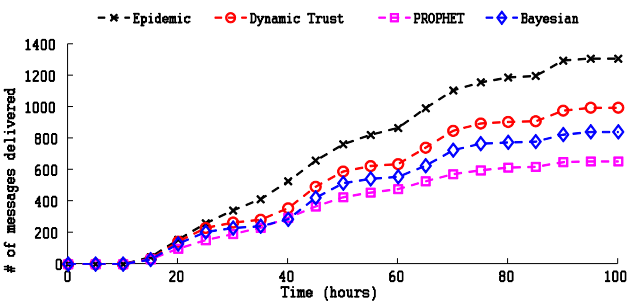


(c) Message Delay.

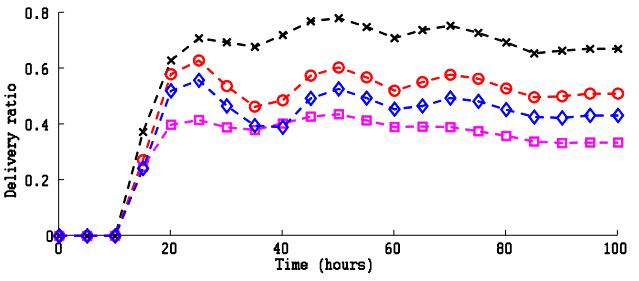


(d) Message Overhead.

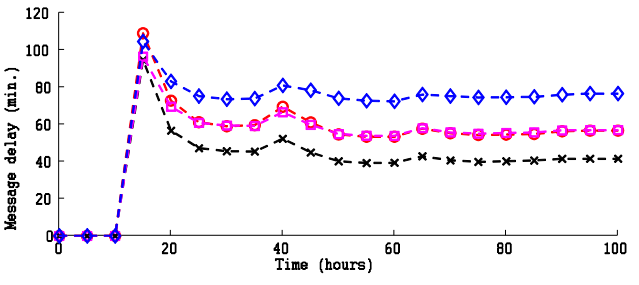
Figure 5: Performance Comparison of Routing Protocols based on SWIM Mobility in Dynamic DTN Environments.



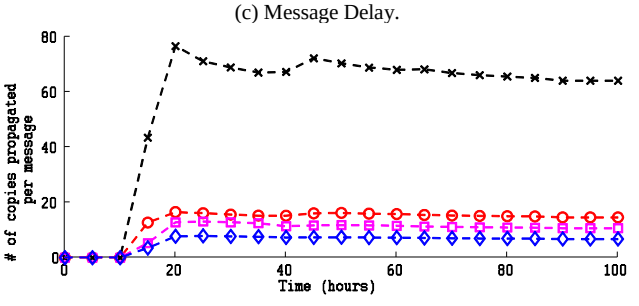
(a) Number of Delivered Messages.



(b) Delivery Ratio.



(c) Message Delay.



(d) Message Overhead.

Figure 6: Performance Comparison of Routing Protocols based on Mobility Traces in Dynamic DTN Environments.

unselfishness trust properties), thus avoiding message forwarding to misbehaving nodes. Moreover, our dynamic trust-based routing protocol operating under the best trust formation setting w^X and the best application-level optimization design setting (T_f, T_{rec}) to maximize the DTN application performance in delivery ratio. We also observe that because the best protocol settings applied are geared toward maximizing the delivery ratio with a delay threshold (set to 2 hours in the experiment), it may lead to a higher message delay compared with other schemes, as only a smaller set of nodes would be selected as message carriers. However we see that when two copies (L=2) are allowed, our dynamic trust-based routing protocol approaches the ideal performance of epidemic routing in delivery ratio and message delay (Figure 5(b)) without incurring high message overhead (Figure 5(c)).

Figure 6 shows performance comparison results based on the *infocom06* mobility trace. We first observe that there are three peak periods in message delivery. This is caused by the three daytime periods in which people are active and most of the messages are delivered. Only a small fraction of the messages are forwarded and delivered during night. The curves in Figure 6 have the same trend as those in Figure 5, thus demonstrating the effectiveness of our dynamic trust management protocol regardless of the mobility pattern. This further validates our dynamic trust management design and its application to DTN routing in real DTN environments.

REFERENCES

[1] The ns-3 Network Simulator, Nov. 2011, http://www.nsnam.org/.

[2] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," *Military Communications Conference*, 2010, pp. 1788-1793.

[3] E. Ayday, H. Lee, and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, Sept. 2012, pp. 1514-1531.

[4] S. Buchegger, and J.-Y. L. Boudec, "Performance Analysis of the Confidant Protocol: Cooperation of Nodes - Fairness in Dynamic Ad-Hoc Networks," *ACM International Symposium on Mobile Ad Hoc Networking and Computing*, June 2002, pp. 226-236.

[5] E. Bulut, Z. Wang, and B. Szymanski, "Cost Effective Multi-Period Spraying for Routing in Delay Tolerant Networks," *IEEE/ACM Transactions on Networking*, vol. 18, no. 5, 2010, pp. 1530-1543.

[6] E. Bulut, Z. Wang, and B. K. Szymanski, "Impact of Social Networks on Delay Tolerant Routing," *IEEE Global Telecommunications Conference*, Honolulu, HI, Nov. 2009, pp. 1-6.

[7] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networking," *IEEE Conference on Computer Communications*, Barcelona, Spain, April 2006, pp. 1-11.

[8] L. Buttyan, L. Dora, M. Felegyhazi, and I. Vajda, "Barter Trade Improves Message Delivery in Opportunistic Networks," *Ad Hoc Networks*, vol. 8, no. 1, 2010, pp. 1-14.

[9] A. Chaintreau, P. Hui, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Impact of Human Mobility on Opportunistic Forwarding Algorithms," *IEEE Transactions on Mobile Computing*, vol. 6, no. 6, July 2007, pp. 606-620.

[10] M. Chang, I. R. Chen, F. Bao, and J. H. Cho, "Trust-Threshold Based Routing in Delay Tolerant Networks," *5th IFIP International Conference on Trust Management*, Copenhagen, Denmark, June 2011, pp. 265-276.

[11] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Trust Management for Encounter-Based Routing in Delay Tolerant Networks," *IEEE Global Communications Conference*, Miami, Florida, USA, Dec. 2010, pp. 1-6.

[12] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," *IEEE Transactions on Parallel and Distributed Systems*, 2013.

[13] J. H. Cho, A. Swami, and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, 2011, pp. 562-583.

[14] E. M. Daly, and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, May 2009, pp. 606-621.

[15] M. K. Denko, T. Sun, and I. Woungang, "Trust Management in Ubiquitous Computing: A Bayesian Approach," *Computer Communications*, vol. 34, no. 3, 2011, pp. 398-406.

[16] G. Dini, and A. L. Duca, "A Reputation-Based Approach to Tolerate Misbehaving Carriers in Delay Tolerant Networks," *15th IEEE Symposium on Computers and Communications*, Riccione, Italy, June 2010, pp. 772-777.

[17] A. Jøsang, and R. Ismail, "The Beta Reputation System," *Bled Electronic Commerce Conference*, Bled, Slovenia, June 17-19 2002, pp. 1-14.

[18] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, 2012, pp. 607 - 640.

[19] S. Kosta, A. Mei, and J. Stefa, "Small World in Motion (SWIM): Modeling Communities in Ad-Hoc Mobile Networking," *7th IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Boston, MA, USA, June 2010.

[20] J. Leguay, A. Lindgren, J. Scott, T. Friedman, and J. Crowcroft, "Opportunistic Content Distribution in an Urban Setting." pp. 205-212.

[21] N. Li, and S. K. Das, "RADON: Reputation-Assisted Data Forwarding in Opportunistic Networks," *2nd ACM International Workshop on Mobile Opportunistic Networking*, Pisa, Italy, Nov. 2010, pp. 8-14.

[22] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *IEEE Conference on Computer Communications*, San Diego, CA, March 2010, pp. 1-9.

[23] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, 2003, pp. 19-20.

[24] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, USA, Aug. 2000, pp. 255-265.

[25] A. Mei, and J. Stefa, "Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals," *IEEE International Conference on Distributed Computing Systems*, Genoa, Italy, June 2010, pp. 488-297.

[26] P. Michiardi, and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *IFIP TC6/TC11 Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, 2002, pp. 107-121.

[27] A. Piyatumrong, P. Bouvry, F. Guinand, and K. Lavangnananda, "Trusted Spanning Trees for Delay Tolerant Mobile Ad Hoc Networks," *IEEE Conference on Soft Computing in Industrial Applications*, 2008, pp. 131-136.

[28] I. Psaras, L. Wood, and R. Tafazolli, *Delay-/Disruption-Tolerant Networking: State of the Art and Future Challenges*, Dept. of El. Eng., University of Surrey, 2009.

[29] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau. "CRAWDAD data set Cambridge/haggle (v. 2009-05-29)," May 2009, http://crawdad.cs.dartmouth.edu/cambridge/haggle.

[30] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNs," *IEEE Conference on Network Protocols*, Orlando, FL, USA, Oct. 2008, pp. 238-247.

[31] C. Song, and Q. Zhang, "COFFEE: A Context-Free Protocol for Stimulating Data Forwarding in Wireless Ad Hoc Networks," *IEEE Communictions Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Rome, Italy, June 2009, pp. 1-9.

[32] A. Vahdat, and D. Becker, *Epidemic Routing for Partially Connected Ad Hoc Networks*, Technical Report, Duke University, 2000.

[33] Z. Xu, Y. Jin, W. Shu, X. Liu, and J. Luo, "SReD: A Secure Reputation-Based Dynamic Window Scheme for Disruption-Tolerant Networks," *IEEE Military Communications Conference*, Boston, MA, Oct. 2009, pp. 1-7.

[34] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. S. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, Oct. 2009, pp. 4628-4639.