Workshop on Privacy, Security and Trust in Mobile and Wireless Systems at 20th IEEE International Conference on Computer Communications and Networks,ICCCN, Maui, Hawaii, July 31, 2011

On Secure Multi-copy based Routing in Compromised Delay Tolerant Networks

Eyuphan Bulut and Boleslaw K. Szymanski
Department of Computer Science and Network Science and Technology Center
Rensselaer Polytechnic Institute, 110 8th Street, Troy, NY 12180, USA
{bulute, szymansk}@cs.rpi.edu

***Abstract*—Routing in delay tolerant networks (DTNs) is challenging due to their unique characteristics of intermittent node connectivity. Different protocols (single-copy, multi-copy, erasure-coding-based etc.) utilizing store-carry-and-forward paradigm are proposed to achieve routing of messages in such environments by opportunistic message exchanges between nodes that are in the communication range of each other. The sparsity and distributed nature of these networks together with the lack of stable connectivity between source destination pairs make these networks vulnerable to malicious nodes which might attempt to learn the content of the messages being routed between the nodes. In this paper, we consider DTNs in which malicious nodes are present, to which we refer to as compromised DTNs. We discuss and analyze the effects of presence of malicious nodes in the compromised DTN on routing of messages. We propose a two period routing approach which aims to achieve desired delivery ratio by a given delivery deadline in presence of malicious nodes. Our results show that, with proper parameter setting, the desired delivery ratio by a given delivery deadline can be achieved most of the time by the proposed method.**

I. Introduction

Delay Tolerant Networks (DTNs) are wireless networks in which at any given time instance, the probability that there is an end-to-end path from a source to destination is low. There are many examples of such networks in real life including wildlife tracking sensor networks [1], military networks [2] and vehicular ad hoc networks. Since the standard routing algorithms assume that the network is connected most of the time, they fail in routing of packets in DTNs.

To handle the sporadic connectivity of nodes in DTNs, *store-carry-and-forward* paradigm is used in routing. That is, if a node has a message copy but it is not connected to (i.e. not in the range of) another node, it stores the message until an appropriate communication opportunity arises. Then, if the encountered node is assessed to be useful for delivery, the message is either forwarded or copied[1] to that node. Several routing algorithms utilizing this paradigm are proposed for DTNs based on flooding and erasure coding techniques. Since flooding based schemes suffer from huge overhead of bandwidth and energy consumption due to redundant transmissions, controlled flooding algorithms which use limited number of copies for each message have been developed. Moreover, single-copy based algorithms in which messages are forwarded towards the nodes which are predicted to have higher probability of meeting with destination are also proposed.

Despite many remarkable studies proposing routing algorithms for DTNs, very few of them consider the security, trust and privacy issues in their designs. However, DTNs are very vulnerable to possible malicious node behavior because of its low node density and lack of stable end-to-end paths between source destination pairs. In this paper, we focus on compromised delay tolerant networks in which malicious nodes are present. We discuss and analyze the effects of presence of malicious nodes in the compromised network on efficient routing of messages. We also propose a two period routing approach which aims to achieve a desired delivery ratio by a given delivery deadline in presence of malicious nodes[2].

The remaining of the paper is organized as follows. In Section II we present the related work while Section III describes our network model and the corresponding assumptions. In Section IV, we discuss and analyze the effects of malicious node behavior on routing under different trust models and network environments. We also elaborate on our two period routing approach and evaluate its performance through simulations. In Section V, we discuss the features of the currently proposed approach and outline the future work. Finally, we offer conclusion in Section VI.

This research was sponsored by US Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-09-2-0053. The views and conclusions contained in this document are those of the authors, and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory or the U.S. Government. The US Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

[1]Note that forwarding and copying of a message to an encountered node is different. If a node forwards the message to an encountered node, it does not keep the copy of the message but in copying it keeps the copy of the message.

[2]We use attacker and malicious interchangeably throughout the paper.

II. Related Work

A. DTN Routing Algorithms

Routing algorithms for delay tolerant networks can generally be classified as: single-copy, multi-copy (replication based) and coding based algorithms. In single-copy based routing [3], [4], a message is forwarded to an encountered node if the delivery metric (computed depending on social relations [5], [6], contact frequency [7] etc.) of that encountered node offers higher delivery probability than the current carrier. In multi-copy based algorithms, multiple copies (limitless [8] or limited [9]) of the message are generated and distributed to other nodes (referred to as relays) in the network. Then, any of these nodes, independently of others, try to deliver the message copy to the destination. In coding based algorithms (erasure coding [10], [11] or network coding [12]), a message is converted into a large set of code blocks such that any sufficiently large subset of these blocks can be used to reconstruct the original message. As a result, a constant overhead is maintained and the network is made more robust against the packet drops when the congestion arises. However, those algorithms introduce computation as well as communication overhead resulted from coding, forwarding, and reconstructing of code blocks.

All of the above algorithms try to achieve average high delivery ratio for messages in different ways. They have advantages and disadvantages over each other in different network environments. However, they all assume friendly network environments which might not be realistic in many real-life DTN scenarios.

B. Security of DTN Routing

Recently, some researchers have studied the security of DTN routing. In [13], Burgess et al. show that replication based DTN routing algorithms are intrinsically fault-tolerant and robust against a large number of attacks even without authentication mechanisms. On the contrary, in a more recent study [14], it has been shown that some specific combinations of attacks can reduce the delivery ratio remarkably.

In [15] and [16], encrypted encounter tickets are proposed to prevent claiming of forged encounter history by malicious nodes. However, these methods cannot detect packet drops in the malicious nodes. Moreover, to detect the blackhole nodes and prevent them from attracting data from the network, different reputation based mechanisms are utilized. In [17], a trusted third-party examiner node called ferry node (which moves around in the network) is introduced. In [18] the history of packet exchange records between nodes are used and in [19] and [20], the feedback mechanisms are used to increase the reputation of nodes which previously had a role in the delivery of packets. Similarly, a trust based mechanism for encounter based routing is proposed in [21].

All of the mentioned above previous studies attempt to secure routing by detecting the individual nodes behaving maliciously and preventing them from obtaining the messages in the network. They consider the malicious behavior only from the attacker's point of view and do not consider the trust among the current network members and their ability to collectively mistrust the attacker. Still, even the currently trustworthy nodes can be open to influence of malicious or attacker nodes which might appear in the network later. Moreover, the current approaches consider the messages to be successfully delivered even if they passed via malicious nodes (in single-copy based routing) or a copy of the message is obtained by any of them (in multi-copy based routing). Yet, exposure of the content of the messages to attackers often significantly lowers or negates the value of its delivery to the destination in many DTN applications (e.g. military, financial).

In this paper, we define the secure delivery as follows:

Definition 1 *Secure delivery: The message is securely delivered to its destination if and only if the message is received by the destination before the deadline and before any attacker receives it*[3].

Note that, this definition differs from the one used in previous work that basically considers only delivery of the message to its destination but not its exposure to attackers.

III. Network Model and Assumptions

Delay tolerant networks are characterized using different mobility models. Random models (e.g. random direction, random waypoint), community-based models [23] and real DTN trace-driven models (e.g. zebranet[1]) are among the most popular ones. We analyze the effect of malicious nodes and coalition of nodes in the network with these malicious nodes on the secure delivery using a limited multi-copy based routing algorithm such as Spray and Wait [9]. Hence, we assume the network environment as described in [9][4].

We assume that there are M nodes randomly walking on a $\sqrt{N}$ x $\sqrt{N}$ 2D torus according to a random mobility model (which makes the intermeeting time between two nodes exponentially distributed). Each node has a transmission range R and all nodes are identical. The buffer space at each node is assumed to be sufficiently large that no message is ever dropped because of lack of storage (this is practical since the proposed algorithm uses fewer copies of the message). The communication between nodes is assumed to be perfectly separable, that is, any communicating pair of nodes do not interfere with any

[3]In multi-copy based routing, once the destination receives the message, it starts an epidemic like acknowledgment and informs other nodes carrying the message copy about delivery. Then, these nodes delete the message copies from their buffer. Since, this epidemic like acknowledgment takes very short time compared to data delivery (as shown in [22]), to simplify analysis, we currently assume that the acknowledgment delay is negligible.

[4]Analysis of secure delivery in community based and real DTN trace-driven models is the subject of our future work.

other simultaneous communication (which is most often the case in DTNs due to sparse node density).

In Spray and Wait [9] algorithm, in normal network conditions, each source node distributes a limited number of copies (L) of its message to other nodes in the network and wait for the delivery of one of them to the destination. If there is no malicious nodes in the network, source node can find the minimum number of copies [9] that it needs to distribute to other nodes to achieve a desired delivery rate (d_r) within a given time constraint (t_d) or delivery deadline by computing[5]:

$$\begin{aligned} L_{min} &= \arg\min\{1 - e^{-\lambda L t_d} \geq d_r\} \\ &= \left\lceil \frac{\ln(1-d_r)}{-\lambda t_d} \right\rceil \end{aligned}$$

where, λ is the rate of exponentially distributed intermeeting times of nodes.

However, delay tolerant network environments in real life may be hostile and due to the sparse network topology and intermittent connectivity, malicious nodes can easily attack the network and degrade the routing and delivery performance of these networks. These malicious nodes can even join the network for a short time and form coalition with the existing nodes. Moreover, it is also reasonable to expect that some nodes in such sparsely connected networks can be open to coalitions. Military based DTNs are good example of such networks. Even though all actors (i.e. soldiers) initially follow only their commander, all may have a level of trustworthiness beyond which they may be convinced to cooperate with unauthorized people.

A high school network is another example. Students in the same class are more likely to be good friends with each other, so their relations are on average more trustworthy than the relations between the students in different classes. Consequently, the best strategy for a student to deliver its message to a specific student outside of her class is to propagate the message to the first classmate of that student met during the class break. However, if she let all students (including the ones out of her class who may not be in as good relationship with her as her classmates) carry the message, she might risk the secrecy of her message, as less trustworthy carriers might reveal the message to a teacher or public in general.

The objective of secure routing is to deliver the messages with a desired delivery ratio by the given deadline but in more secure ways, without revealing the message content to malicious nodes. Thus, we discuss the ways of distributing the message copies to relay nodes based on their trustworthiness levels and propose a two period spreading in which initially the message is spread only to trusted nodes, and only in the second spraying period it is shared with more risky nodes.

[5]Since only a limited number copies (L) of the message during delivery is used and these copy counts are much smaller than the total node count in the network ($L << M$), as it is shown in [22] and [9], $1-e^{-\lambda L t_d}$ is a good approximation of delivery probability. However, a more complex analysis could be made by taking into account the spraying phase duration.

IV. Proposed Protocol, Analysis and Results

In this section, we discuss and analyze the secure delivery of messages in compromised delay tolerant networks where the nodes in the network might be open to coalition with malicious nodes. We first define the trust model used throughout the paper:

Definition 2 *Trust model: The nodes are assumed to be trusted by the source, from whom they received the messages, with a probability of p_t that this trust is justified. Thus, when a node of this level of trust carrying a message copy meets the attacker, it gives the message copy to attacker node with probability $p = 1 - p_t$.*

We analyze two variants of trust distribution among the nodes and discuss the effect of different message distribution schemes on secure delivery.

A. Constant Trust Model

Here, assuming that all nodes are trusted by the source node with a constant probability p_t of trust correctness, we analyze the effects of attackers on secure delivery and find out the L_{min} number of copies of a message needed to achieve a desired delivery ratio d_r by deadline t_d.

Theorem 1 *For a given d_r, t_d, λ (rate of exponentially distributed intermeeting time between nodes), n (number of attackers), and $p = 1 - p_t$, the minimum number of copies that must be distributed to the network is:*

$$L_{min} = \left\lceil \frac{\ln(1 - d_r(pn+1))}{-\lambda t_d(pn+1)} \right\rceil$$

Proof: We first find the cumulative distribution function of secure delivery when there are L copies of the message under the given network environment. Let X be the random variable (r.v.) representing the secure delivery. Then cumulative distribution function of X, $F_X(x)$, is:

$$F_X(x) = P(X \leq x) = \int_0^t L\lambda e^{-L\lambda x}(e^{-Lpn\lambda x})dx$$

Here, the first term ($L\lambda e^{-L\lambda x}$) shows the probability density function (pdf) of the meeting probability of any of the L nodes (carrying a message copy) with destination and the second term ($e^{-Lpn\lambda x}$) shows the cdf of the non-meeting probability of any of these L nodes with any attacker node. This is a consequence of the definition of secure delivery, which requires the delivery of a message copy to destination before attacker gets it. Then:

$$\begin{aligned} F_X(x) &= \int_0^t L\lambda e^{-L(pn+1)\lambda x} \\ &= \frac{1}{pn+1}(1 - e^{-L(pn+1)\lambda t}) \end{aligned}$$

n\p	0.2	0.4	0.6	0.8	1.0
1	0.83	0.71	0.62	0.55	0.50
2	0.71	0.55	0.45	0.38	0.33
3	0.62	0.45	0.35	0.29	0.25

TABLE I
MAXIMUM ACHIEVABLE SECURE DELIVERY RATIOS WITH DIFFERENT CONSTANT TRUST PROBABILITIES AND ATTACKER COUNTS.

Thus, equation for L_{min} that can achieve d_r by t_d becomes:

$$L_{min} = \left\lceil \frac{\ln(1 - d_r(pn+1))}{-\lambda t_d(pn+1)} \right\rceil$$

■

Note that, in the above $F_X(x)$ formula, it is clear that the maximum value of $F_X(x)$ is $1/(pn+1)$ (which becomes $1/(n+1)$ when $p = 1$). Thus, if the deadline of delivery is not an issue, attacker count decides the maximum achievable delivery rate. Table I shows these maximum achievable secure delivery ratios with different constant trust probabilities and attacker counts. We also verified these results through simulations on a simple network environment details of which are given in the next section.

B. Group-based Trust Model

The trust levels of nodes in a network may also be group-based, making the distribution of message copies more challenging. We need to answer the following question: "what should the spraying strategy be for a given trust distribution of nodes in the network?".

A source node, having the objective of delivering its messages to their destinations without revealing them to attackers, may use one the following message distribution strategies:

- Fully Trusted Spraying (FTS): Source node sends the message copies to its fully trusted friends only. Even though this strategy makes the routing of messages completely secure, delivery delay might increase if only few nodes are trusted.
- Aggressive Spraying (AS): Source node sprays the message copies to nodes it encounters first. With this strategy, the number of message copy carriers increases quickly in the network, improving chances of delivery, but message copies might be distributed to either partially trusted or even untrusted nodes, increasing the probability of revealing the message to attackers.
- Trusted First Spraying (TFS): Source node distributes the message copies to the nodes in the network in the order of their trust levels. Thus, first the message copies are distributed to fully trusted friends. Once all trusted nodes have a message copy, message is copied to partially trusted nodes. Finally, after all trusted and partially trusted friends have the message copy, untrusted nodes are given the message copies.

Each of the above strategies might be advantageous compared to others in different network environments and with different delivery objectives. In addition to the above three trivial strategies, we propose a fourth and a novel way of spraying:

- Two Period Spraying: The message copies are distributed to the network in two steps. In the first period, the source copies the messages only to trusted nodes. In the second period, any encountered node is selected. In other words, source starts with secure spraying and switches to aggressive spraying with the start of the second period.

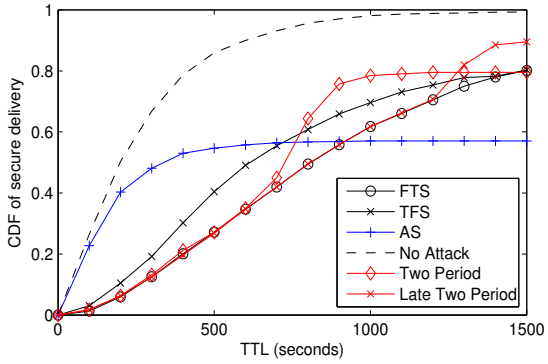

Fig. 1. Cumulative distribution function of secure delivery ratios in different spraying algorithms.

Next, we will show the performances of these algorithms on a sample network environment. We deployed $M = 100$ mobile nodes onto a torus of size 300 m by 300 m. All nodes are assumed to be identical and their transmission range is set to $R = 10$ m (note that these parameters generate a sparse delay tolerant network which is the most common case in practice). The movements of nodes are decided according to random walk model. The speed of a node is randomly selected from the range [4, 13]m/s and its direction is also randomly chosen. Then, each node goes in the selected random direction with the selected speed until the epoch lasts. Each epoch's duration is randomly selected from the range [8, 15]s. With nodes move according to this model with the given above parameters the intermeeting time between any two pairs of nodes is 480s.

We generated three groups of nodes with different trust levels. Only 5% of all nodes in a network are fully trusted by source node ($p_t = 1$) and 20% of nodes are trusted with probability of p_t=0.7, meaning that when they have message copies and the attackers meet with them, they give the message copy to attacker with probability $p = 1 - p_t = 0.3$. The remaining nodes in the network are not trusted ($p_t = 0$), thus they give the message copy to the attackers ($p = 1$) in case they meet with them.

Figure 1 shows the cumulative distribution function of secure delivery ratios (with respect to the time since the generation of messages at source nodes (TTL)) when the aforementioned spraying algorithms are used. We considered a single attacker in the system. It is clear that

when there is no attackers, the maximum delivery ratio is achieved. When there is an attacker, the delivery ratio of aggressive spraying increases fast but it can only reach the maximum which is around 0.5. The delivery ratio of FTS increases slowly but since the source node gives the copies only to nodes that do not give the message copy to attackers, the delivery ratio has potential of reaching the maximum value of 1. This algorithm might be preferable since it preserves privacy, however if achieving a higher delivery ratio within a time constraint is an objective, it is not the best choice. Looking at the graph of TFS, we notice that the delivery ratio increases faster than the delivery ratio of FTS, but it eventually converges to a constant value since it risks the privacy of the message while using partially trusted nodes. Those nodes contribute to delivery ratio in earlier stages but since they might form coalition with attacker, in long term their benefit is lost. Note that the spanned delivery ratios by the plots of these three algorithms (TFS, FTS, AS) clearly indicate that each of these algorithms might be preferred depending on the given network parameters (desired delivery ratio, deadline). However, one can have a goal of achieving a delivery rate that cannot be achieved by any of these algorithms. For those cases, we propose to use two period spraying idea. Consider the delivery ratios achieved in two different runs of two period spraying algorithm. The only difference between these two runs is the start of second period of spraying. Clearly, the start of second period can be chosen according to the network parameters.

Theorem 2 *When there are L_t trusted nodes carrying the copy of the message in the first period and L_u partially trusted nodes with probability $p_t = 1-p$ that start to carry a message copy in second period (making in total $L_a = L_u + L_t$ nodes with a copy), to achieve a given d_r (with no t_d), the start of second period, t_2, must be larger than a constant, t_2^{min}, where:*

$$t_2^{min} = \frac{-\ln\left((1-d_r)(\frac{L_a}{npL_u}+1)\right)}{\lambda L_t}$$

Proof: Let X_2 be the r.v. representing the secure delivery in two period spraying. In the first period, $F_{X_2}(x)$ grows with $1-e^{-\lambda L_t x}$. But if the delivery does not happen in first period (with probability $e^{-\lambda L_t t_2}$) and second period starts, the pdf of secure delivery in second period is supported by L_a nodes towards delivery and risked by L_u partially trusted nodes. Thus, $F_{X_2}(x)$ in second period becomes:

$$\begin{aligned} F_{X_2}(x) &= 1 - e^{-\lambda L_t t_2} + e^{-\lambda L_t t_2}(S) \text{ where} \\ S &= \int_0^{x-t_2} L_a \lambda e^{-L_a \lambda x}(e^{-L_u np \lambda x})dx \\ &= \frac{L_a}{L_a + npL_u}(1 - e^{-(L_a+npL_u)\lambda(x-t_2)}) \end{aligned}$$

In the above formula, maximum delivery ratio that can be reached (when x goes to ∞) is $1 - e^{-\lambda L_t t_2}\left(\frac{npL_u}{L_a+npL_u}\right)$. Since this value must be larger than d_r, minimum value of the start of the second period can be derived as:

$$t_2 \geq \frac{-\ln\left((1-d_r)(\frac{L_a}{npL_u}+1)\right)}{\lambda L_t}$$

■

Corollary 1 *For a given parameter set (L_t, L_u, t_2), the cdf of delivery rate in FTS is definitely better than the cdf of delivery rate in two period spraying after t_{max}, where:*

$$t_{max} = t_2 + \frac{\ln(1 + \frac{L_a}{L_u np})}{\lambda L_t}$$

which can be easily proved by comparing the maximum achievable delivery ratio of two period spraying with the cdf of delivery ratio of FTS algorithm.

If there is a time constraint, t_d, and the goal is to achieve the maximum possible delivery rate (which is not achievable by FTS) with given L_u, then the start of the second period could be adjusted accordingly.

Theorem 3 *For a given delivery deadline, L_u and L_t, the optimal value of t_2 that gives the maximum delivery rate by t_d is t_2^{opt}, where:*

$$t_2^{opt} = t_d + \frac{\ln\left(\frac{L_t npL_u}{L_a(L_a+npL_u-L_t)}\right)}{\lambda(L_a + npL_u)} \quad (1)$$

Proof: We first find $d'(t_2) = \frac{F_{X_2}(t_d)}{d(t_2)}$ and $d''(t_2) = d'(t_2)/d(t_2)$:

$$\begin{aligned} d'(t_2) &= \lambda(e^{-\lambda L_t t_2})\left[L_t\left(\frac{npL_u}{L_a + npL_u}\right) + \right. \\ &\quad \left. (L_t - L_a - npL_u)e^{-\lambda(L_a+npL_u)(t_d-t_2)}\right] \end{aligned}$$

Then, solving $d'(x) = 0$, we obtain:

$$x = t_d + \frac{\ln\left(\frac{L_t npL_u}{L_a(L_a+npL_u-L_t)}\right)}{\lambda(L_a + npL_u)}$$

Since, $d''(x) < 0$, $F_{X_2}(t_d)$ has local maximum at x, making $t_2^{opt} = x$. ■

In addition to time constraint, if there is a desired delivery rate, d_r (again which is not achievable by FTS), and minimizing the average cost of the algorithm (average number of message copies sprayed to network) is also another objective, the start of second period and the number of untrusted nodes, L_u, that will carry a message copy in second period must be selected carefully.

Theorem 4 *For a given delivery deadline, t_d, and desired delivery rate, d_r, the optimal number of untrusted nodes*

that minimize the overall routing cost which still achieves d_r by t_d can be computed as in Algorithm 1.

Proof: Cost of the algorithm can be computed as:

$$\begin{aligned} c(L_t, L_u) &= L_t(1 - e^{-\lambda L_t t_2}) + (L_t + L_u)e^{-\lambda L_t t_2} \\ &= L_t + L_u e^{-\lambda L_t t_2} \end{aligned}$$

We first find the first L_u that achieves a secure delivery rate higher than desired d_r by t_d. Then, if the achieved delivery rate is much higher than d_r, we delay the start of second period as much as possible (without dropping delivery rate below d_r) because with constant L_t and L_u, the cost of the algorithm decreases with the increase of t_2. To find such t_2, we can use binary search between t_2^{opt} and t_d. ■

Finding the closed form of exact optimum t_2 that achieves d_r by t_d will be the subject of our future work.

Algorithm 1 Find Optimum Routing(L_t, p, n, d_r)

1: $L_u = 1$
2: Find $t_2^{opt}(L_u)$ from Eq. 1
3: **while** $(F_{X_2}(t_2^{opt}) < d_r)$ **do**
4: $\quad L_u = L_u + 1$
5: $\quad$ Find $t_2^{opt}(L_u)$ from Eq. 1
6: **end while**
7: **if** $(L_t + L_u e^{-\lambda L_t t_2^{opt}} > d_r)$ **then**
8: $\quad$ Find exact $t_2^{opt\_exact}$ by binary search in $[t_2^{opt}(L_u), t_d]$
9: **end if**
10: $opt\_L_u = L_u$; $opt\_cost = L_t + L_u e^{-\lambda L_t t_2^{opt\_exact}}$

Note that, the above algorithm finds L_u that gives the optimum cost when a given constant L_t nodes can not achieve d_r by t_d. However, if there are sufficient trusted nodes (L_t) to achieve these goals, only they are used without using untrusted ones.

V. Discussions and Future Work

A. Complex Functional Trust Models

In this paper, we only considered constant and group-based trust models. However, the trust distribution of nodes might be more complex than the introduced ones. That is, all nodes of the network may be open to coalition with attackers, but with different probabilities (maybe according to a given function). Then, the distribution of message copies becomes a much more challenging problem. Consider Figure 2, where we plot three different trust level distributions of nodes in a network. These three plots represent the generalized views of any possible trust distribution when sorted in descending order. The complete analysis of the performance of introduced algorithms in these trust models will be subject of future work, however, in our first explorations, we have discovered that two period protocol could be more beneficial in trust-prone network environments.

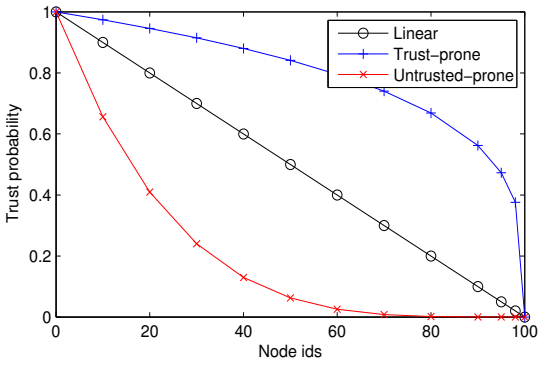

Fig. 2. Different trust level distributions.

B. Real DTN Traces

Recently, many projects focused on the deployment of real delay tolerant networks in several network environments (office [24], conference [25], city [26]) using different mobile objects (human [27], bus [28], zebra [1]). According to the collected trace data from these deployments, it has been discovered that the characteristics of DTNs and also the mobility of mobile objects might be more complex than the random models. Thus, we plan to analyze the proposed algorithms in these heterogeneous network environments in our future work. We can model such a problem as follows:

Assume that source node s has intermeeting frequency rate of λ_{si} with node i. Moreover, assume that the trust level of node i is t_i. The question is for a given set of λ_{si} and t_is for all nodes in the network ($0 \leq i \leq N$), what is the optimal message distribution scheme that provides the maximum secure delivery rate by a given deadline?

C. Online Behavioral Trust Computation

We currently assumed that the trust distribution of other nodes (to source node) is already computed or known by the source node. However, how each node can compute the trust levels of other nodes is another goal in our future plans. We plan to use behavioral trust mechanisms such as the one proposed in [29]. Moreover, we would like to integrate feedback mechanisms to the trust computation such that nodes on previous delivery paths (of source's messages) earn extra trust levels.

VI. Conclusion

In this paper, we focused on the problem of routing in compromised delay tolerant networks in presence of malicious nodes. Assuming that, with certain probability, the nodes in the network are open to coalition with these malicious nodes, we discussed and analyzed several message distribution schemes in terms of secure delivery of messages. We also proposed a novel method of two period spraying in which routing of messages is risked when the remaining time to delivery deadline gets closer.

By our initial simulations and analysis, we showed that two period spraying protocol achieves better delivery ratio at later times which can not be achieved by other methods. We believe that our secure delivery definition with the proposed two period spraying protocol will lead to a new studies of the routing problem in delay tolerant networks with limited trust between nodes (compromised DTNs).

References

[1] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, *Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet*, in Proceedings of ACM ASPLOS, 2002.

[2] *Disruption tolerant networking*, http://www.darpa.mil/ato/solicit/DTN/.

[3] J. Burgess, B. Gallagher, D. Jensen, B. N. Levine, *Maxprop: routing for vehicle-based disruption-tolerant networking*, in Proceedings of INFOCOM, 2006, pp. 1-11.

[4] E. Bulut, S. Geyik and B. Szymanski, *Efficient Routing in Delay Tolerant Networks with Correlated Node Mobility*, in Proceedings of 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), Nov, 2010.

[5] E. Daly and M. Haahr, *Social network analysis for routing in disconnected delay-tolerant manets*, Proc. ACM MobiHoc, 2007.

[6] E. Bulut, B. Szymanski, *Friendship based Routing in Delay Tolerant Mobile Social Networks*, in Proceedings of Globecom 2010, Miami, December 2010.

[7] A. Lindgren, A. Doria, and O. Schelen, *Probabilistic routing in intermittently connected networks*, SIGMOBILE Mobile Computing and Communication Review, vol. 7, no. 3, 2003.

[8] A. Vahdat and D. Becker, *Epidemic routing for partially connected ad hoc networks*, Duke University, Tech. Rep. CS-200006, 2000.

[9] T. Spyropoulos, K. Psounis,C. S. Raghavendra, *Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-copy Case*, IEEE/ACM Transactions on Networking, 2008.

[10] Y. Wang, S. Jain, M. Martonosi, and K. Fall, *Erasure coding based routing for opportunistic networks*, in Proceedings of ACM SIGCOMM workshop on Delay Tolerant Networking (WDTN), 2005.

[11] E. Bulut, Z. Wang, B. Szymanski *Cost Efficient Erasure Coding based Routing in Delay Tolerant Networks*, in Proceedings of ICC 2010, South Africa.

[12] Y. Lin, B. Li, and B. Liang, *Efficient network coded data transmissions in disruption tolerant networks*, in Proceedings of IEEE INFOCOM, 2008.

[13] J. Burgess, G. D. Bissias, M. D. Comer, and B. N. Levine, *Surviving attacks on disruption-tolerant networks without authentication*, in Proceedings Mobihoc'07, pp. 61-70, 2007.

[14] F. C. Choo, M. C. Chan and E. Chang, *Robustness of DTN against Routing Attacks*, in Proceedings of Second International Conference on Communication Systems and Networks (COMSNETS), pp. 1-10, 2010.

[15] F. Li and J. Wu, *Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets*, in Proceedings of INFOCOM, pp. 2428-2436, 2009.

[16] S. C. Nelson, M. Bakht and R. Kravets, *Encounter-based Routing in DTNs*, in Proceedings of IEEE Infocom, Rio De Janeiro, Brazil, pp.846-854, Apr. 2009.

[17] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, *Muton: Detecting malicious nodes in disruption-tolerant networks*, in Proceedings of WCNC, 2010.

[18] Y. Ren, M. C. Chuah, J. Yang, Y. Chen, *Detecting blackhole attacks in disruption-tolerant networks through packet exchange recording*, in Proc. of 1st Workshop D-SPAN (colocated with WoWMoM), 2010.

[19] G. Dini and A. L. Duca, *A reputation-based approach to tolerate misbehaving carriers in delay tolerant networks*, in Proceedings of 15th IEEE Symposium on Computers and Communications, Italy, 2010.

[20] N. Li, S. K. Das, *RADON: reputation-assisted data forwarding in opportunistic networks*, in Proceedings of MobiOpp, pp. 8-14, 2010.

[21] I. R. Chen, F. Bao, M. J. Chang, and J. H. Cho, *Trust Management for Encounter-based Routing in Delay Tolerant Networks*, IEEE Global Communications Conference, Miami, USA, Dec. 2010.

[22] E. Bulut, Z. Wang, B. Szymanski, *Cost Effective Multi-Period Spraying for Routing in Delay Tolerant Networks*, in IEEE/ACM Transactions on Networking, vol. 18, 2010.

[23] T. Spyropoulos, K. Psounis,C. S. Raghavendra, *Performance Analysis of Mobility-assisted Routing*, MobiHoc, 2006.

[24] S. Srinivasa and S. Krishnamurthy, *CREST: An Opportunistic Forwarding Protocol Based on Conditional Residual Time*, in Proceedings of SECON, 2009.

[25] A European Union funded project in Situated and Autonomic Communications, *www.haggleproject.org*.

[26] J. Leguay, A. Lindgren, J. Scott, T. Friedman, J. Crowcroft and P. Hui, *CRAWDAD data set upmc/content (v. 2006-11-17)*, downloaded from http://crawdad.cs.dartmouth.edu/upmc/content, 2006.

[27] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, *Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms*, in Proceedings of INFOCOM, 2006.

[28] X. Zhang, J. F. Kurose, B. Levine, D. Towsley, and H. Zhang, *Study of a Bus-Based Disruption Tolerant Network: Mobility Modeling and Impact on Routing*, In Proceedings of ACM MobiCom, 2007.

[29] S. Adali, R. Escriva, M. Hayvanovych, M. Magdon-Ismail, B. Szymanski, W. Wallace and G. Williams, *Measuring Behavioral Trust in Social Networks*, IEEE International Conference on Intelligence and Security Informatics (ISI 2010) pp. 150 - 152, Vancouver, BC, May 23 - 26, 2010.