Robustness of DTN against Routing Attacks

Fai Cheong Choo
Dept of Computer Science
National University of Singapore
Email: faicheon@comp.nus.edu.sg

Mun Choon Chan
Dept of Computer Science
National University of Singapore
Email: chanmc@comp.nus.edu.sg

Ee-Chien Chang
Dept of Computer Science
National University of Singapore
Email: changec@comp.nus.edu.sg

***Abstract*—In this work, we study robustness of DTN routing in the absence of authentication. We identify conditions for an attack to be effective and present an attack based on a combination of targeted flooding and acknowledgement counterfeiting that is highly effective even with only a small number of attackers. Simulation results show that delivery ratio decrease by 30% to 50% using only 2 attackers for the two mobility patterns studied (Haggle and DieselNet). We observe that minimum hop count for packet delivery has a strong influence on the robustness of the DTN routing protocols. Generally, attacks become increasingly effective when the minimum hop count required increases. Further, use of global routing metadata in the routing protocol also increases attack effectiveness. Our study provides insights to the robustness of routing attacks in different DTNs settings and can be useful to DTN designers who want to choose the appropriate level of security that is needed for their respective scenarios.**

I. Introduction

Delay Tolerant Networks (DTNs) are a class of networks in which there may be no contemporaneous path between the source and destination at a given time. Packet delivery over a DTN is often characterized by large end-to-end path latency and a DTN routing protocol has to deal with frequent disconnections.

In order to improve the performance of DTN routing, a number of mechanisms have been utilized in different DTN routing protocols [1], [2], [3], [4], [5], [6]. These mechanisms often include replication of packets to many nodes so as to increase the chances of delivery and to reduce the delivery latency. In a single contact, only limited packets may be exchanged between two mobile nodes. As a result, the order of packet transfer, which depends on the priority a node associates with each packet, has significant impact on the overall performance. Replication-based DTN routing protocols differ mainly on how each packet's priority is determined.

In addition to the routing protocol used, a DTN performance can also be affected by attacks from malicious nodes. Existing works on MANET routing security that focus on securing the path establishment process [7], [8], [9], [10], [11], [12] cannot be use for securing DTN as DTN routing are typically opportunistic with no end-to-end path establishment.

Many approaches for securing routing in DTN depend on using public key cryptography to limit participants to a set of authorized nodes and using class of service for the allocation of buffering and link capacity [13], [14], [15], [16]. Such approaches include authenticating every routing metadata and packets at every intermediate hop, incurring considerable processing overhead. In addition, key management may not be easy to carry out under certain trust models and scenarios, and is further complicated by the sporadic connectivity of DTN.

Recent work has suggested that some DTNs coupled with replication-based routing protocols are intrinsically fault-tolerant, and robust against a large number of malicious attackers even in the absence of authentication [17]. This poses the question of the necessity of authentication or the level of authentication required especially since authentication imposes overhead. Without authentication, the number of nodes willing to join the network may actually increase due to the easier deployment, resulting in better overall performance.

In this paper, we revisit and study the robustness of DTNs without authentication. We present an attack based on a combination of targeted flooding and acknowledgement counterfeiting. We quantify the effectiveness of our attacks on UMass DieselNet and Haggle trace which have previously been thought to be robust when a replication-based routing protocol (MaxProp) is used [17]. The proposed combination attack is highly effective, even when only a small number of attackers are used. Simulation shows that delivery ratios decrease by 30% to 50% using only 2 attackers for the two mobility patterns studied.

We observe that minimum hop count for packet delivery has a strong influence on the robustness of the DTN routing protocols. Generally, attacks become increasingly effective when the minimum hop count required increases. An observation we make in this work is that the small number of hops needed to deliver a packet in some DTNs (DieselNet and Haggle) is one of the reasons why they are robust against the routing attacks in [17].

The use of globally flooded routing metadata in the routing protocol to guide routing decision also increases attack effectiveness. Routing protocols such as MaxProp[5] and Rapid[6] uses globally flooded routing metadata to guide routing and buffer management decision. However, due to the flooded nature of the routing metadata, it makes the attackers easy to spoof and flood tainted routing metadata. We show in section IV-A1 that a very small number of attackers can taint the routing metadata of a large number of nodes. Hence, a large number of nodes can be misguided by the tainted routing metadata, degrading routing performance.

Our study provides insights into the effectiveness of routing attacks in different DTN settings and can be useful to DTN designers who want to decide on the level of security that is

978-1-4244-5489-1/10/ $26.00 © 2010 IEEE

appropriate for their respective scenarios.

The rest of the paper is organized as follow. Section II presents related work. In Section III, we present the security and mobility model assumed, and the routing protocol used for evaluation. Section IV present details on the proposed routing attacks. Evaluation is presented in Section V and we conclude in Section VI.

II. Background

Current approaches for securing routing in DTN largely depends on using public key cryptography to limit participants to a set of authorized nodes and using class of service for buffer space and link capacity allocation [13], [14], [15], [16]. In addition, every routing metadata and packets injected into the network are authenticated at every intermediate hops. Such approaches incur considerable overhead and have to deal with the difficulty of key management.

Public keys can be pre-distributed before deployment, but this approach is more difficult to realise when incremental deployment of network nodes is desirable. Alternatively, a public key infrastructure (PKI) may be used. However, in disconnected environments such as DTN, access to online servers for fetching public keys or checking Certificate Revocation Lists (CRL) may not be possible.

Recently, Identity-Based Cryptography (IBC) schemes have been proposed for use in DTN environments[15][16]. With IBC scheme, the recipient public key is simply a function of a public identification string of the recipient, hence the recipient identity implicitly validate the recipient public key. Furthermore, instead of checking the Certificate Revocation Lists (CRL), time-based keys are used for revoking the rights of compromised or malicious nodes. Such schemes however, still require all nodes in the network to trust and register with the Private Key Generator (PKG). The PKG must be able to verify that the node is indeed allowed to use the public identifier. A confidential communication channel will be needed to securely deliver the private key to the node.

While routing security has been studied extensively in traditional ad hoc networks [7], [8], [9], [10], [11], [12], the work cannot be easily extended to DTN due to different routing style and network characteristics. For example, route in traditional ad hoc networks are mainly established before any data transfer. Routing disruption attacks such as black hole[7], [8], flood rushing[12] and wormhole[9] attack the route establishment process. It either causes route establishment to fail, or establishes a route that will not be able to deliver the data. In DTNs where routing is opportunistic, there is typically no path establishment before sending data.

Our work is closely related to Burgess's work [17] on the robustness of DTN against attackers in the absence of authentication. The benefits of DTN without authentication include less processing overhead, no administrative difficulty and more attractive to get nodes to join the network. Having more nodes in the DTN provide more contact capacity and buffer for the network. As noted by Burgess et al, for many non-military scenarios, it is unlikely that a network will attract a large percentage of attackers. Hence if DTN can withstand a small percentage of attackers, it may be more beneficial to forgo authentication so as to attract more participating nodes. The main question is whether DTN without authentication is robust enough against a small percentage of attackers.

While Burgess's work suggests that some DTNs coupled with replication-based routing protocols are intrinsically fault-tolerant and robust against a large percentage of attackers, it remains unclear why the protocols are robust or the scenarios whereby DTNs will be robust against the attackers.

In this work, we present an attack that is effective against replication-based DTN routing protocols and identify scenarios where DTNs are most vulnerable to such an attack.

III. System Model

In this section, we describe the security assumptions, mobility models used and properties of the routing protocol evaluated.

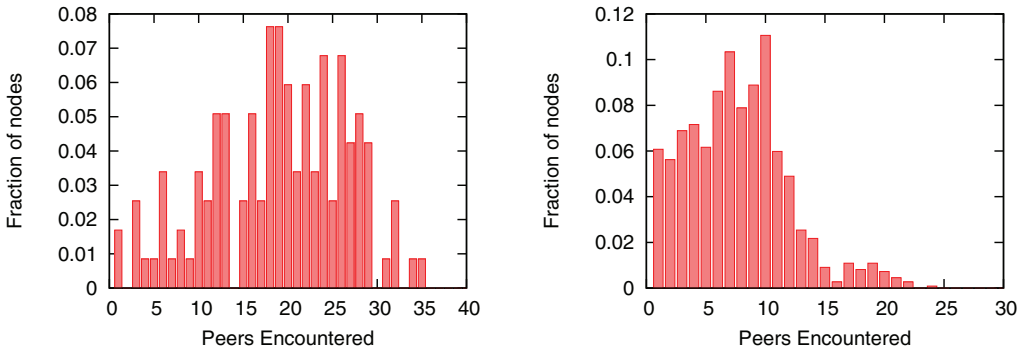
A. Security Assumptions

We assume that nodes do not perform authentication of relay nodes in the network. Similarly, no authentication is performed on the authenticity of messages. As a result, attackers can spoof their MAC layer addresses to appear to be any node, including destinations of packets. Routing metadata and packets can also be spoofed and relay nodes have no means to verify their authenticity.

Finally, we also assume that attackers do not have global knowledge of DTN topology and future transfer opportunities. Stronger attackers with global knowledge and choice of location will be able to inflict much more damage than our attacker model here. However, we show that even with a weaker attacker model, attackers can still degrade the performance of the network considerably such that we need to be wary about DTNs without authentication.

B. Mobility Models

Our evaluation are based on real network traces, namely the DieselNet [5] and Haggle project [18] traces which are similarly used in [17]. The Haggle trace consists of a 3 day long trace that is based on a human mobility experiment in Infocomm 2005. A total of 41 volunteers joined the experiment and each was given an iMote device that can communicate with one another using Bluetooth. The iMotes are also capable of connecting to other Bluetooth-capable devices in the environment. Similar to the experiment in [17], we removed connection events from the Haggle data that lasted less than one second or involved the singular appearance of a node since meaningful data transfer is likely to require setup time and nodes incapable of routing data may be ignored. After the transformation, the traces left with only events involving 41 Class 1 devices (the iMotes devices) and none of the Class 2 devices (other Bluetooth-capable devices). In order to limit a single simulation interval to be 24 hours or less, we split the Haggle trace into 3 segments, each lasting about 1 day.



(a) Haggle (b) DieselNet

Fig. 1. Unique Peers Encountered Daily

The DieselNet trace comprises of roughly 30 buses (with specific number varying according to the bus schedule). The median number of DieselNet buses in each trace is 19. Buses are outfitted with wireless transmitters and receivers. Communication between the buses is performed via the 802.11b protocol. DieselNet trace consists of 60 days of traces (captured during January to May 2005).

Figure 1 shows the number of peers encountered per mobile node for the two traces. Nodes in the Haggle trace have a broader distribution of peers encountered. The median number of peers contacted by each node in the Haggle trace is 19, about 45% of the network. The median number of peers contacted by each node in DieselNet is 7, about 39% of the median number of buses in each trace.

C. Routing Model

The routing protocol used in our evaluation is MaxProp [5], a replication-based DTN routing protocol. MaxProp has been shown to provide robustness against various attacks [17]. It offers better throughput than several other strategies such as Epidemic [1], Prophet [3], Spray and Wait [2] and even Dijkstra algorithm with an oracle of future transfer opportunities [19].

While we use MaxProp in our study, our study is applicable to other replication-based routing protocols that use flooded routing metadata to guide replication and buffer management.

In terms of packet scheduling/replication, MaxProp replicates packets in the following order:

1) Packets destined to the directly connected node
2) Routing metadata (estimations of the probability of meeting every other node)
3) Acknowledgements of delivered data.
4) Packets in ascending order of hop count for hop count below a certain threshold. This threshold is adaptive and is determined by using the average contact capacity measured from previous encounters.
5) Packets in descending order of delivery likelihood.

In terms of buffer management, MaxProp removes packets from its buffer in the following order:

1) Acknowledged packets.
2) Packets in ascending order of delivery likelihood for packets with hop count above a certain adaptive threshold.
3) Packets in descending order of packet hop count.

MaxProp uses network-wide acknowledgements to remove delivered packets from relay and source nodes, clearing up buffer and also prevent nodes from receiving packets which have already been delivered. The acknowledgements are created when packet reaches the destination and the acknowledgements are flooded throughout the network.

As mentioned by Burgess et al [17], to mitigate the effects of acknowledgement counterfeiting, a node should ignore an acknowledgement if it has not seen the packet being acknowledged beforehand. In all our experiments, we implement this defense against acknowledgement counterfeiting.

In MaxProp and many similar DTN routing protocols [3], [4], [5], [6], routing metadata is exchanged and kept when two peers meet. Each node maintains a copy of its own table that describes the node contacts that it has observed in the past. Each table has an associated timestamp, indicating the time in which the table was last updated. These contact information or routing metadata is replicated to other nodes during contact so that other nodes are aware of each others' contact history. When two nodes in the contact have different versions of the routing metadata entry, the copy with the earlier timestamp will be replaced. Figure 2 shows an example of MaxProp routing metadata that is stored at node A.

Based on the routing metadata exchanged, the data maintained in each contact table is used to estimate delivery likelihood. In the case of MaxProp, the delivery likelihood is computed in the form of path cost. The higher the delivery likelihood, the lower the path cost. The cost of the path $i, i+1, ..., d$ is the sum of the probabilities that each connection on the path does not occur: $c(i, i+1, ..., d) = \sum_{x=i}^{d-1} \left[1 - \left(f_{x+1}^{x}\right)\right]$. In figure 2, the most likely path for delivering a packet from A to D is through node B, since the path cost ABD is the minimum. The cost is computed as ABD=0.3 ((1 - 0.9) + (1 - 0.8)).

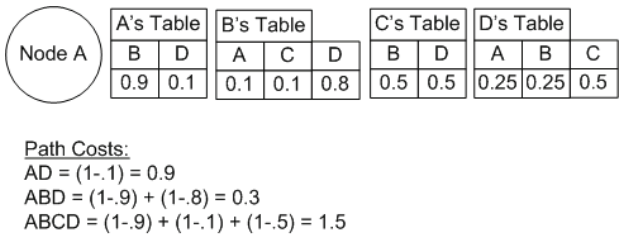


Fig. 2. The organization of routing metadata in a node

IV. Motivation and Proposed Attack

In [17], four general attacks *Drop All*, *Random flooding*, *Invert routing metadata*, and *Acknowledgement counterfeiting* were experimentally shown to be ineffective.

Drop All attack is not effective as there are still many possible paths to destination that do not involve the attackers.

In Random flooding attack, the priority to replicate or drop the attackers' packets is the same as non-attackers' packet. Hence the effectiveness of Random flooding attack is limited by how fast the attackers can inject packets into the network to cause resource contention.

For Invert routing metadata attack, it attempt to cause the list of packets to be transmitted or drop in the reverse order. Its effectiveness is limited by how resource constrained the network is. For example, if two peers meet and they have enough contact capacity to transmit all their buffer contents to the other node, then even if the list of packets are transferred in the reverse order, there is no performance degradation at all. Perhaps a more severe limitation of invert routing metadata attack is that simply inverting every routing metadata may not be effective. If an attacker sees the same routing metadata the second time, inverting it the second time gives correct version of the routing metadata.

In Acknowledgement counterfeiting, attackers must first know the existence of a packet before it can fake acknowledgements. Its effectiveness is limited by how quickly the attackers know the existence of a packet.

While the above attacks may be ineffective, many variations of these attacks are still possible. Furthermore, these attacks can be combined to reinforce each other.

A. Proposed Attack

Our proposed attack combines and uses a variation of the above attacks in an attempt to overcome the described limitations. It consists of two components. The first component, called *non-deliverable packet flooding* floods data to non-existent nodes to cause resource contention. It also includes *routing metadata falsification* that spoof routing metadata so that the flooded packets gets higher priority in replication and lower priority in being dropped. The second component *identity impersonation* impersonates different identities to act as destinations for packets. Furthermore, upon knowing the existence of a packet, attackers flood network-wide acknowledgements of the packet in an attempt to purge the packet out from the network.

The primary purpose of the first component is to cause network resource congestion, and to make relay nodes having a higher tendency to drop non-attackers' packets from their buffer and replicate attackers' packets. The second component aims to purge packets from both the source and the relay nodes. We explain in detail the two components in the following sections.

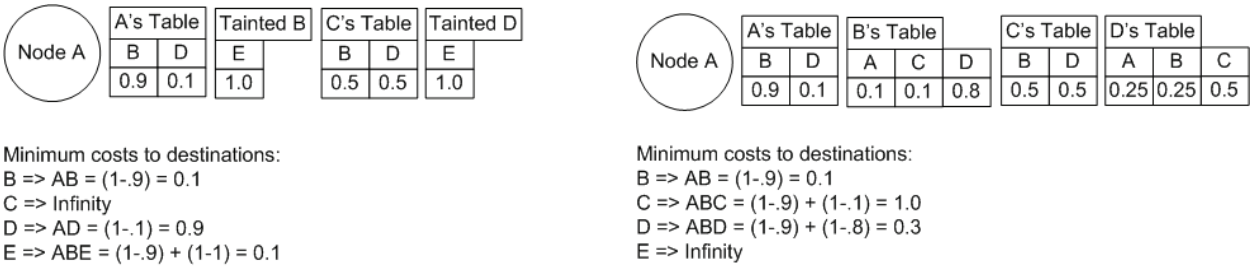
1) Non-Deliverable Packet Flooding: In non-deliverable packet flooding attack, attacker floods new packets to some non-existent destinations so that the flooded packets will not be delivered and stay in the network for a long period of time. However, with MaxProp and other routing protocols that rely on contact histories to estimate delivery time or probability, non-deliverable packets are actually given the lowest priority. These packets are replicated last and in the case of buffer contention, they will be dropped first. This is undesirable from the attacker's point of view. To counter that, attackers can perform routing metadata falsification by spoofing every node's routing metadata and claim that the node can reach the non-existent destination with high probability. More specifically in our experiments, the attackers remove all entries in a routing metadata table and create an entry with meeting probability 1 to the non-existent destination.

Figure 3 shows node A's routing metadata with and without routing metadata attack. Node E is a non-existent destination and attackers flood packets to node E. With routing metadata attack, node A will give replication priority for packets in the order B, E, D, C. Further, if there is contention for buffer, packets destined to C will be dropped first. Without routing metadata attack, node A will give replication priority for packets in the order B, D, C, E and if there is contention for buffer, packets destined to E will be dropped first. This illustrates that routing metadata attack can successfully raise the priority of the attackers' flooded packets.

Effectiveness of metadata falsification

Consider an attack where N_A attackers keep injecting false routing information of a victim node, say node D. Let's call a node who is neither an attacker nor the victim a *carrier* node. Whenever an attacker meets a carrier node, it will send a *tainted* table (see Figure 3 for example) of node D, which contains false information and time-stamped with the latest time. On the other hand, the victim also injects the correct table to the carrier nodes. Recall that whenever two nodes meet, they will exchange and update their routing metadata to the one with the later timestamp. Note that only the attackers and victim will set the timestamp, carrier nodes simply help replicate the routing metadata without modifying the timestamp.

Now, under the above spreading process, we want to determine the fraction of carrier nodes having the tainted table. We claim that the fraction is $N_A/(N_A+1)$ under reasonable assumptions. Let us consider this mobility model: The time is divided into periods of unit length. During each period, two randomly chosen nodes come into contact. The random nodes chosen in each period are independent to choices made in other periods. Let $X_{t,i}$ be the random variable where $X_{t,i} = 1$ if



(a) Under Attack (b) Without Attack

Fig. 3. Comparison of node's routing metadata with/without attack.

the node i's metadata is tainted at time t, and 0 otherwise. For convenience[1], let us assume that initially (i.e. at time 0), each node has the probability of $N_A/(N_A+1)$ being tainted (i.e. $Prob(X_{0,i}=1) = N_A/(N_A+1)$). We can show that, for any i and $t \geq 0$,

$$E(X_{t,i}) = \frac{N_A}{N_A+1}. \quad (1)$$

From (1) and linearity of expectations, the fraction of carrier nodes having a tainted table over all carrier nodes is also N_A/N_A+1. To show (1), let us consider a carrier node whose routing metadata originates from a malicious node or the victim, and trace back how the routing metadata spread from the source. We say that there is a path from node p_0 at time t_0 to node p_1 at time t_1, if there is a sequence

$$j_1 = p_0,\ s_1 = t_0,\ j_2, s_2, j_3, \ldots, j_{k-1}, s_{k-1} = t_1,\ j_k = p_1,$$

where node j_i and j_{i+1} meet during time period s_i, and the subsequence $s_1, s_2, \ldots$, is strictly increasing. Let us take $(t_1 - t_0)$ as the length of the path. Note that if there is a path from node p_0 to the victim, and it is shorter than every path to a malicious node, then the metadata in p_0 will not be tainted. Similarly, if there is a path to a malicious node, and every path to the victim is longer, then the metadata will be tainted. Due to the independencies in choosing the two nodes in each time period, the probability that the nearest node is malicious is $N_A/(N_A+1)$.

To know the effectiveness of routing metadata falsification in the Haggle and DieselNet traces, we perform simulations on them to get the fraction of nodes having a tainted routing metadata. Each simulation was run till the end of the trace and the fraction of nodes having a tainted routing metadata is noted. The result presented here is the average of the different runs of the simulation. The description of these traces and simulations can be found in section III-B. Figure 4 shows that the traces in our simulation exhibit similar fraction of tainted nodes compared to our stochastic model here.

The result in figure 4 suggests that it is possible for very few attackers to launch an effective routing metadata falsification attack. This apply even for large networks with hundreds or thousands of nodes. Hence, we expect our non-deliverable packet flooding attack to benefit much from the use of routing metadata falsification.

[1]This assumption on the initial condition is not crucial. One may consider the initial condition where all metadata are untainted. In this case, the fraction approaches $N_A/(N_A+1)$, instead of the equality we obtained in (1).

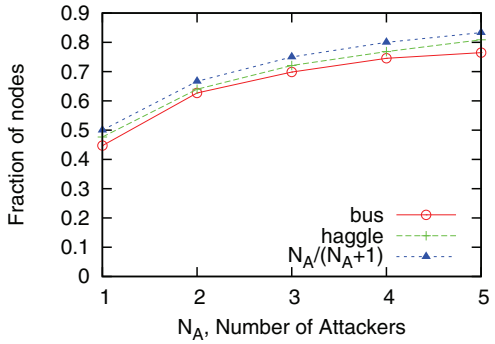


Fig. 4. Fraction of nodes with tainted routing metadata

2) Identity Impersonation Attack: In the identity impersonation attack, attackers impersonate different identities to act as destinations for packets so as to trick relay nodes or the packet source node to believe that the packets have been delivered. Furthermore, upon knowing the existence of a packet, attackers flood network-wide acknowledgements of the packet into the network. Nodes that are tricked into believing that the packets have been delivered will drop the packets from their buffer.

Such attack directly exploits the lack of node authentication. In a single contact, an attacker can potentially take on the identities of many other nodes if the contact duration is sufficiently long. In the extreme case, all packets in a node's buffer can be falsely removed. This is possible since frequent disconnections are the norms in DTN. This attack is most effective when the attacker encounters the source early in the packet forwarding process when the number of replicas of a packet in the network is low.

V. Evaluation

We evaluate the robustness of DTNs in the presence of attackers launching random flooding attacks (rf), non-deliverable packet flooding attacks (ndp), and identity impersonation attack (imp). For identity impersonation attack, we limit the switching of identity to at most once per second. All our evaluations were performed using our simulator that was

modified from the ONE simulator[20], a simulator developed specifically for DTN simulations.

The traces used for simulation are the Haggle and DieselNet trace (see section III-B for description). In our simulation, we randomly assign nodes as honest and attacker nodes. All honest nodes generate traffic destined for other randomly chosen honest nodes. Each node has a 5MB buffer size and packets may be deleted before delivery when the buffer is full. When a packet is to be dropped due to buffer full, a node will always drop packets originating from other nodes before considering dropping its own packets. In all simulations, packets are fixed at size 10KB. Whenever load is too high, delivery rate is very low due to contention. In order to isolate the effects of the attackers, we use a moderate packet load of 10 packets/hr per honest node. Finally, in the identity impersonation attack, we assume that a malicious node can take on a new identity only once every second.

The transfer capacity of a single contact has an impact on the routing performance. In the Haggle trace, only contact duration is provided. If we assume the bluetooth device can transmit at 1Mbps, the median per-contact capacity will be approximately 25MB. In all our evaluations, we set the median per-contact capacity to be 25MB, including the DieselNet trace. Figure 5 shows the CDF graph of the per-contact capacity for the Haggle and DieselNet trace. In this setting, there is greater than 80% of the contact opportunities having enough capacity to transfer the full buffer contents of the two meeting nodes. The main resource contention here is hence the buffer.

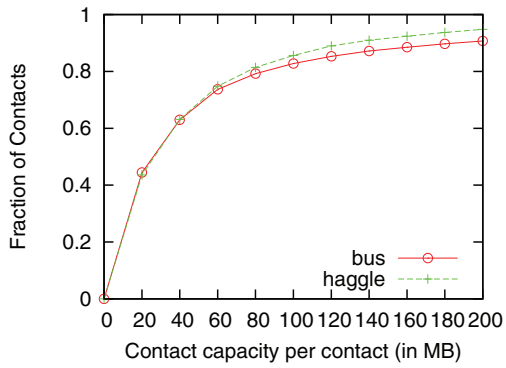


Fig. 5. CDF of contact capacity

A. Evaluation varying attackers

From figure 6-8, it can be seen that non-deliverable packet flooding is effective even when there are only 1-2 attackers. In fact, the addition of more attackers does not help to bring the delivery ratio much lower. The reason is that 1-2 attackers is enough to cause the relay nodes' buffer to be filled with the attackers' packets due to the replicative nature of MaxProp protocol and high per-contact capacity. Further, since the packets are non-deliverable, they stay in the relay nodes' buffer for a long period of time, causing contention with other relay packets. For random flooding, there is less buffer contention since flooded packets may be delivered to the destination quickly, and these are removed from the relay nodes' buffer much faster. Furthermore, unlike non-deliverable packet flooding attack, random flooding attack does not manipulate the routing metadata to give the attackers' packets higher priority to stay in the buffer or be selected for replication. Note that in the simulation, nodes always keep packets originating from it. Hence even though relay packets are dropped, the source node still holds a copy of the packet and can still deliver the message through direct contact with the destination. Non-deliverable packet flooding fails to attack such direct contact delivery situation.

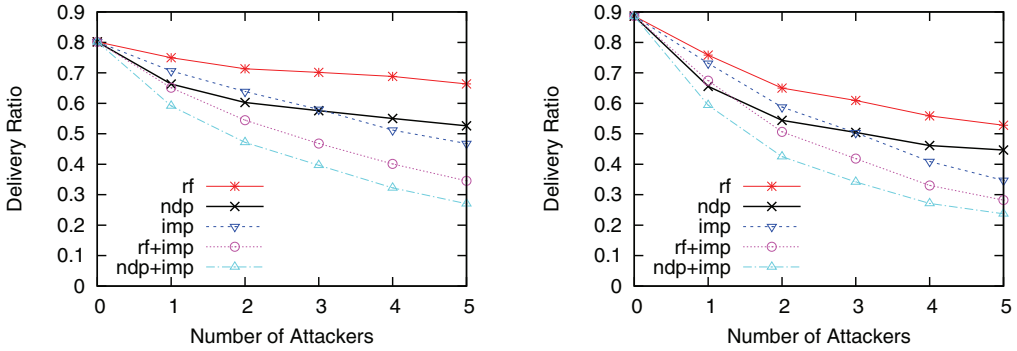
Figure 7 shows the hop count of messages at the time they were delivered to their destinations with 10% attackers. It can be seen that without flooding attacks, there are quite a number of packets delivered with 3-6 hop counts. On the other hand, with flooding attacks, most packets tend to be delivered with only 1 or 2 hop counts. The main reason is that flooding causes many packets to be dropped at relay nodes due to buffer contention. Since in our simulation, source always give higher priority in keeping its own packets, and due to mobility, the source may later meet the destination of the packets and send the packets to it directly. In other words, the capability of each node to eventually meet many other nodes provides substantial robustness against flooding attacks that causes packets to be dropped at relay nodes. Note however, the delivery latency is affected by flooding attacks, causing much higher delivery latency as shown in Figure 8.

Unlike non-deliverable packet flooding, impersonation attack is more effective when the number of attackers increases since launching the attack requires direct contact. The more attackers there are in the network, the more performance degradation it causes. Flooding attack and impersonation attack are complementary and can be launch together to cause more damage, as can be seen from figure 6.

B. Communicating Pairs Evaluation

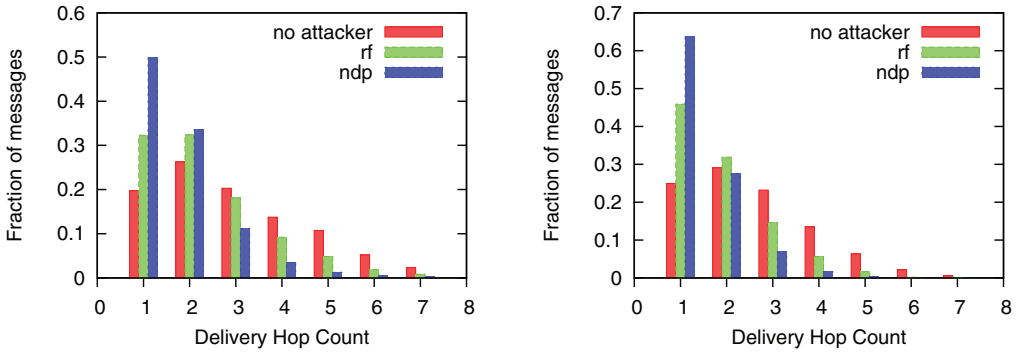
In this section, we evaluate the routing performance of peers who are communicating across different distances (in terms of hop count required). Our goal is to understand how non-deliverable packet flooding and identity impersonation attack affect communicating peers that communicate over different distances in terms of hop counts. We first use a synthetic trace to better understand the effects of the attacks followed by further evaluation on the Haggle and DieselNet traces.

The synthetic trace imposes some structure so that it is possible to evaluate peers communicating with different number of minimum hop counts required. It consists of 40 nodes in a 5 by 5km area. The 40 nodes are divided into 8 different groups (each group consist of 5 nodes), and each node in a group move around an attraction point in the map with a standard deviation of 500m. The position of attraction points are randomly generated with the constraint that no two attraction points are within 1000m to each other. We generate 10 such synthetic traces for our simulation and the results reported are the averaged of the 10 traces.



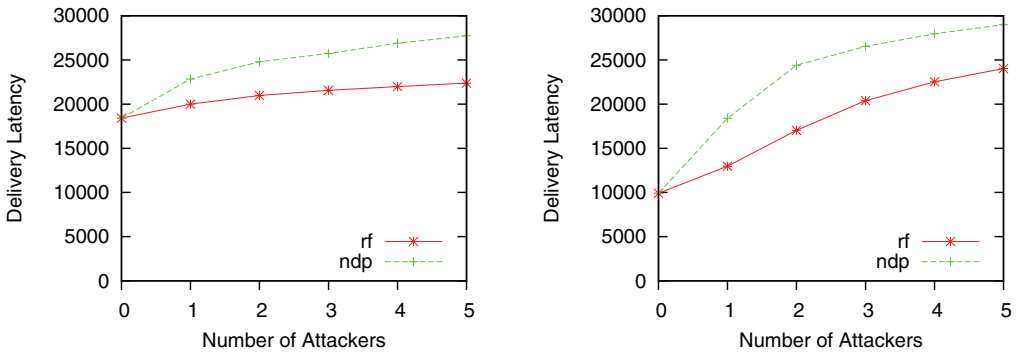
(a) Haggle (b) DieselNet

Fig. 6. Delivery Ratio under buffer contention



(a) Haggle (b) DieselNet

Fig. 7. Message hop count at delivery (10% attackers)



(a) Haggle (b) DieselNet

Fig. 8. Delivery Latency under buffer contention

In our evaluation of attacks, we place one attacker in one of the groups, call it group A. We want to evaluate the delivery ratio when an honest node in a group sends packets to another honest node in a certain group.

We divide the communicating pairs into the following category:

1) A-A: packets sent from a node in group A to another node in group A
2) A-B: packets sent from a node in group A to another node in group B. Group B's attraction point is at most 2000m from group A's attraction point.
3) A-C: packets sent from a node in group A to another node in group C. Group C's attraction point is at least 2000m away from group A's attraction point.
4) X-Y: packets sent from a node in group X to another node in group Y where there is no attacker in group X and Y. In addition, group X's attraction point is at least 2000m away from group Y's attraction point.

Figure 9 shows the distribution of hops taken when packets are delivered in each category when there are no attackers. Majority of the packets in category A-A are delivered within 1-2 hops. For category A-C, C-A, X-Y and Y-X, the communication is further apart with majority of the packets delivered after going through more than 3 hops.

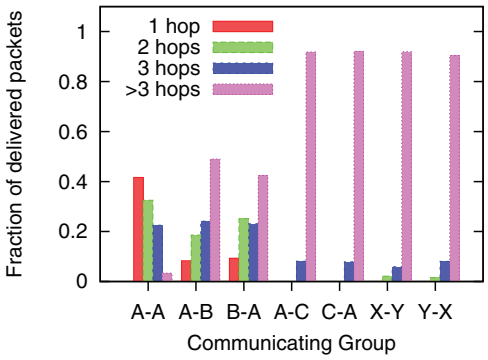


Fig. 9. Distribution of hops taken

Figure 10 shows the delivery ratio of nodes communicating in different groups (recall that 1 attacker is placed in group A). When the number of hops required is low (eg. A-A), non-deliverable packet flooding do not have any effect, since eventually the source node may directly meet the destination node. However, when the number of hops required is high (eg. A-C), communication between the two peers relies on relay nodes. Non-deliverable packet flooding causes relay nodes along the path to drop packets, and the communication in category A-C is severely affected. The delivery ratio drops from 0.77 (without attacker) to 0.09 (one attacker). This demonstrates that for peers that require a few hops in order to communicate, non-deliverable packet flooding attack can have a serious impact on them.

Identity impersonation attack is more effective when the attacker is closer to the source of a packet, giving higher chance that the attacker eliminates the packet before it is replicated to many other nodes. This is especially clear when comparing category A-C and C-A under identity impersonation attack. Delivery ratio for category A-C is only 0.11 compared to 0.46 for group C-A communication.

For group X-Y and Y-X communication, effectiveness of non-delivery packet flooding depends on the location of the attacker. If attacker is far from the communication path of X-Y and Y-X, then it may fail to effectively taint the relay nodes routing metadata. In such cases, relay nodes will then drop the attacker's flooded packets when there is buffer contention. Identity impersonation attack also does not work well in such cases since by the time the attacker learns about the existence of a packet and try to flood counterfeit acknowledgements into the network, the packet may have already been delivered or replicated many times and is close to being delivered.

We now move on to further evaluation using the Haggle and DieselNet trace. Figure 11 shows the delivery ratio based on the minimum hop count required for a packet to be delivered to

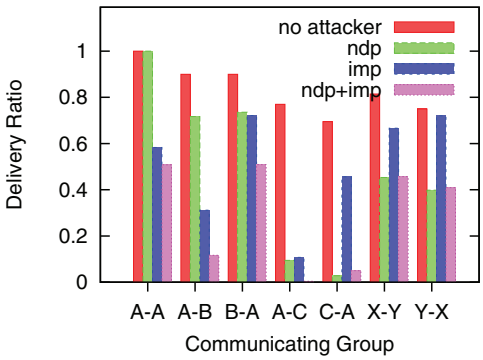


Fig. 10. Communicating pairs evaluation (1 attacker in Group A)

the destination. We did not show the results for minimum hop count that is greater than 3 as the number of these packets are too little. Similar to what we observed in the synthetic trace, packets with high minimum hop count required for delivery are severely affected by non-deliverable packet flooding attack. Packets with minimum hop count of 1 for delivery are not affected by non-deliverable packet flooding attack, but it is still susceptible to identity impersonation attack.

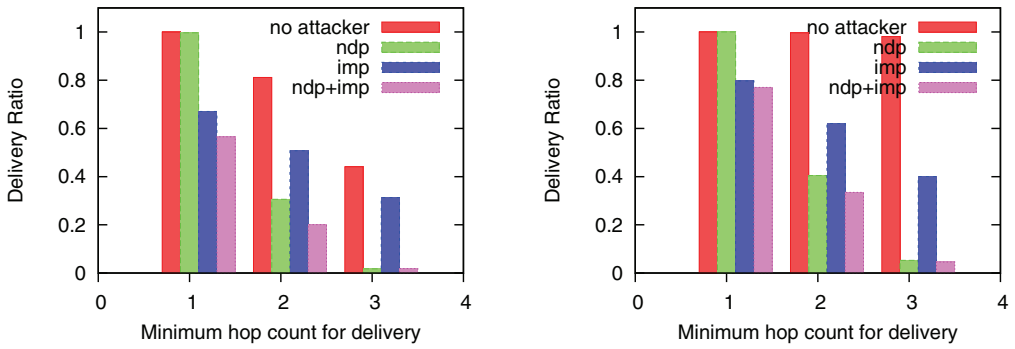
C. Robustness with globally flooded routing metadata

In this section, we evaluate the packet delivery ratio for two routing protocols. The first is MaxProp, which uses globally flooded routing metadata to guide routing decisions. The second is a modification to the MaxProp protocol. We remove the routing metadata used in MaxProp, and the routing decision is solely based on packet hop count. Packets with lower hop counts are given higher priority for replication and lower priority for drop. We call this protocol HC.

Since only the non-deliverable packet flooding attack makes use of falsification of routing metadata, we only perform non-deliverable packet flooding attack here and exclude identity impersonation attack. Figure 12 shows the delivery ratio of the two routing protocols. The delivery ratio of MaxProp degrades much faster than HC. Using packet hop count to guide routing decision is not affected by the routing metadata falsification component of non-deliverable packet flooding attack, hence non-deliverable packet flooding is not effective against HC. Falsifying hop count will be more difficult for attackers, since they will have to see the packet first before being able to modify the hop count.

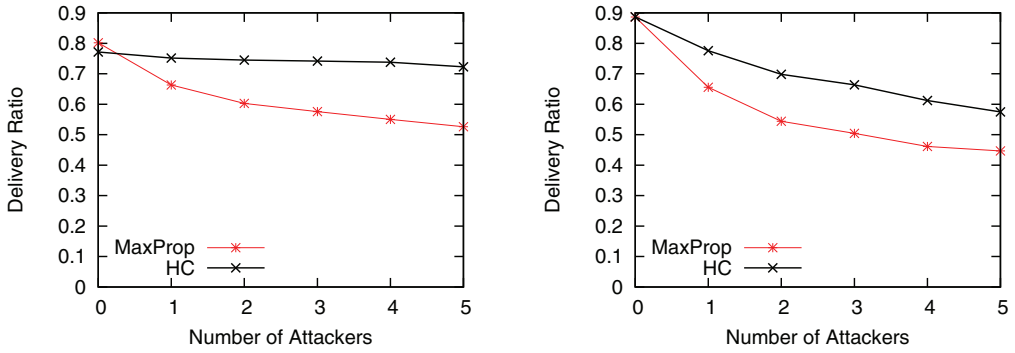
D. Evaluation varying Buffer Size

We investigate whether increasing buffer size makes MaxProp more robust against non-deliverable packet flooding attack. Figure 13 shows that increasing buffer size does not help in making MaxProp more robust against non-deliverable packet flooding attack. Even with additional buffer, the attackers' packets quickly filled up the buffer, causing similar level of resource contention.



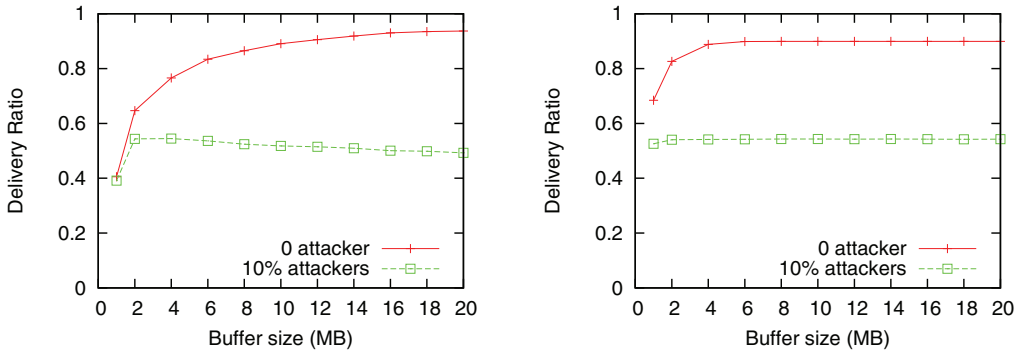
(a) Haggle (b) DieselNet

Fig. 11. Delivery Ratio with different minimum hop count for delivery (10% attackers)



(a) Haggle (b) DieselNet

Fig. 12. Delivery Ratio of MaxProp and HC



(a) Haggle (b) DieselNet

Fig. 13. Delivery Ratio varying buffer size

E. Discussion

Previous sections discussed the attacks without any routing authentication. What if some form of authentication can be performed? We consider two levels of authentication here:

1) Authenticate the identity of the peer in an encounter
2) Authenticate the identity of the peer in an encounter, routing metadata and acknowledgements

In (1), nodes in the network authenticate the peer when there is an encounter. Nodes can easily authenticate each other based on public key in a certificate. Overhead is low but in this case, it only prevent against identity impersonation (partially). The attacker will not be able to impersonate as the destination of packets, but it will still be able to flood fake acknowledgements. Note that non-deliverable packet flooding attack is not affected by such authentication at all. As such, authentication at this level is not effective against our attacks.

In (2), besides authenticating the identity of the peer, it also authenticates the routing metadata and acknowledgements. For acknowledgements, they are signed by the destination node. The overhead involved is much higher compared to (1), but it can fully prevent identity impersonation. As for non-deliverable packet flooding attack, flooding to non-existent destination is still possible. However, the metadata falsification component is thwarted. Hence, non-deliverable packets will be correctly determined by relay nodes that it is unlikely to be delivered. In this case, the relays will choose to drop these packets in the event of buffer contention. As a result, non-deliverable packet flooding will not be effective. It should be noted however, *tailgating* attack can be launch with non-deliverable packet flooding attack. This allows non-deliverable packets to be seen as highly deliverable by relay nodes, enhancing the effectiveness of non-deliverable packet flooding attack. (It is out of the scope of this paper to discuss tailgating attack, reader is referred to the paper [21] for more information.)

VI. Conclusion

Contrary to previous work [17], we show that DTN with replicative routing protocols are not necessarily robust under known denial of service attacks if there are no authentication mechanism in place. Under many networking settings and mobility patterns, carefully designed attacks based on well-known techniques can cause considerable performance degradation. We investigated the attack effectiveness under various settings and identified properties of the networking environment that attribute to the vulnerability of the network. We observed that routing protocols which globally floods routing metadata to guide routing decisions are more susceptible to attacks as the routing metadata can be easily spoofed. We also observed that the minimum hop count required for packet delivery plays an important role. Generally, attacks become increasingly effective when the minimum hop count required increases. For DTNs whose peers need to communicate with high number of hops, the attacks can be highly effective even for very small number of attackers and we believe that authentication mechanism should be in place.

Acknowledgment

This research is supported by the National University of Singapore under grant R-252-000-359-112 and TDSI/09-003/1A.

References

[1] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Department of Computer Science, Duke University, Durham, NC, Tech. Rep., 2000.

[2] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *WDTN '05: Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*. New York, NY, USA: ACM Press, 2005, pp. 252–259.

[3] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *Lecture Notes in Computer Science*, vol. 3126, pp. 239–254, January 2004.

[4] B. Burns, O. Brock, and B. Levine, "Mv routing and capacity building in disruption tolerant networks," vol. 1, 2005, pp. 398–408 vol. 1.

[5] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networking," in *Proceedings of IEEE Infocom 2006*, Barcelona, Spain, April 2006. [Online]. Available: http://prisms.cs.umass.edu/brian/pubs/burgess.infocom2006.pdf

[6] A. Balasubramanian, B. N. Levine, and A. Venkataramani, "DTN Routing as a Resource Allocation Problem," in *Proc. ACM Sigcomm*, Kyoto, Japan, August 2007. [Online]. Available: http://www.sigcomm.org/ccr/drupal/?q=node/273

[7] D. Djenouri and N. Badache, "Struggling against selfishness and black hole attacks in manets," *Wirel. Commun. Mob. Comput.*, vol. 8, no. 6, pp. 689–704, 2008.

[8] D. Hongmei, L. Wei, and A. Dharma P., "Routing security in wireless ad hoc networks," *IEEE Communications magazine*, October 2002.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," vol. 3, 2003, pp. 1976–1986 vol.3.

[10] Cristina and H. Rubens, "An on-demand secure routing protocol resilient to Byzantine failures," in *ACM Workshop on Wireless Security (WiSe)*, Atlanta, Georgia, September 2002.

[11] S. Yi, P. Naldurg, and R. Kravets, "A security-aware routing protocol for wireless ad hoc networks," in *in: Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc)*, 2001, pp. 286–292.

[12] Y. chun Hu, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *in ACM Workshop on Wireless Security (WiSe)*, 2003, pp. 30–40.

[13] K. Fall, "A delay tolerant network architecture for challenged internets," in *Proc. of Annual Conf. of the Special Interest Group on Data Communication (ACM SIGCOMM'03)*, August 2003, pp. 27–34. [Online]. Available: http://citeseer.ist.psu.edu/728928.html

[14] R. Durst, "A infrastructure security model for delay tolerant networks," july 2002. [Online]. Available: http://www.dtnrg.org/docs/papers/dtn-sec-wp-v5.pdf

[15] A. Seth and S. Keshav, "Practical security for disconnected nodes," in *Proceedings of the 1st IEEE ICNP Workshop on Secure Network Protocols*, 2005.

[16] A. Kate, G. M. Zaverucha, and U. Hengartner, "Anonymity and security in delay tolerant networks," in *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, 2007, pp. 504–513.

[17] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, "Surviving attacks on disruption-tolerant networks without authentication," in *MobiHoc '07: Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*. Montreal, Quebec, Canada: ACM Press, 2007, pp. 61–70.

[18] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket switched networks and human mobility in conference environments," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, Philadelphia, PA, USA, August 2005, pp. 244–251. [Online]. Available: http://www.acm.org/sigs/sigcomm/sigcomm2005/paper-HuiCha.pdf

[19] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," August 2004.

[20] A. Keränen and J. Ott, "Increasing reality for dtn protocol simulations," Helsinki University of Technology, Tech. Rep., July 2007. [Online]. Available: http://www.netlab.hut.fi/~jo/papers/2007-ONE-DTN-mobility-simulator.pdf

[21] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Distruption-Tolerant Networks using Encounter Tickets," in *Proceedings of IEEE Infocom 2009*, 2009.