Thwarting Blackhole Attacks in Distruption-Tolerant Networks using Encounter Tickets

Feng Li, Jie Wu
Dept. of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL 33431

Avinash Srinivasan
Dept. of Math, Computer Science, and Statistics
Bloomsburg University
Bloomsburg, PA 17815

***Abstract*—Nodes in disruption-tolerant networks (DTNs) usually exhibit repetitive motions. Several recently proposed DTN routing algorithms have utilized the DTNs' cyclic properties for predicting future forwarding. The prediction is based on metrics abstracted from nodes' contact history. However, the robustness of the encounter prediction becomes vital for DTN routing since malicious nodes can provide forged metrics or follow sophisticated mobility patterns to attract packets and gain a significant advantage in encounter prediction. In this paper, we examine the impact of the blackhole attack and its variations in DTN routing. We introduce the concept of encounter tickets to secure the evidence of each contact. In our scheme, nodes adopt a unique way of interpreting the contact history by making observations based on the collected encounter tickets. Then, following the Dempster-Shafer theory, nodes form trust and confidence opinions towards the competency of each encountered forwarding node. Extensive real-trace-driven simulation results are presented to support the effectiveness of our system.**

***Index Terms*—Blackhole attacks, disruption-tolerant networks (DTNs), encounter tickets, observation, PKI, security, uncertainty**

I. Introduction

Unlike traditional networks, where packets are forwarded along fixed links, disruption-tolerant networks (DTNs) [1] allow packet forwarding along intermittent links. Consequently, traditional stable-link-based routing and packet forwarding protocols are not applicable to DTNs, since a contemporaneous end-to-end path may never exist. Therefore, nodes use an underlying store-and-forward model of routing to cope with unstable paths, usually caused by high mobility and a low density of nodes.

In existing practical DTNs, such as the UMass DieselNet [2], real objects' movements usually follow repetitive patterns. Due to this repetitive nature, future encounters can be estimated based on the gathered history. Routing in DTNs with predicted encounters is an active research area. Existing routing schemes, such as MaxProp [3] and ProPHET [4], use metrics, such as the number of previous encounters the current node has had with other nodes, as the primary factor to evaluate the competency of a forwarding node.

However, these metrics are usually provided by forwarding nodes themselves, and are hard to verify in DTNs due to intermittent links. Besides, commonly used metrics in existing DTN routing schemes, such as the total number of previous encounters in [3] or last encounter time in [5], are too straight forward and easily lend themselves to be forged. In this paper, we propose a robust encounter prediction system that is secure against such malicious nodes.

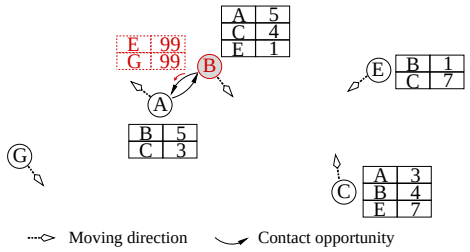


Fig. 1. Blackhole attack. Links denote the existence of previous encounters. B is the attacker. The table beside each node shows the actual number of encounters. B gives A forged numbers of encounters to attract packets.

The unique features of DTNs pose unique security challenges for encounter prediction. One immediate observation is the *blackhole attack* [6], in which a malicious node can provide forged metrics to other nodes that it comes in contact with and attract packets from them. After receiving these forwarded packets, the malicious node can either drop them or utilize them to launch other, more sophisticated attacks. In traditional networks including mobile ad hoc networks (MANETs), nodes have additional evidence, such as geographical, temporal, or structural leashes, to detect and isolate malicious nodes that launch blackhole attacks. However, in DTNs, such evidence is usually either unavailable or difficult to gather. Therefore, in DTNs, it is important to secure the contact evidence to prevent malicious nodes from providing false contact information.

In this paper, we first introduce the notion of *encounter tickets* from the perspective of routing and packet forwarding. When two nodes meet, they generate an encounter ticket that carries a timestamp. Based on a commonly trusted PKI, both nodes sign the ticket with their private keys. In our scheme, when a node reveals its contact history to another node, it is required to submit the encounter tickets instead of a compressed list containing only node IDs and the number of contacts previously employed by other schemes, as shown in Fig. 1. This idea is simple but powerful. It greatly increases the cost incurred by an attacker who launches blackhole attacks, which shall be confirmed by the results presented in Section VII.

Despite enforcing encounter tickets, the attacker can still use advanced techniques such as tailgating to boost its metrics. To thwart such attacks, we propose the ticket-based *history interpretation* scheme. When one node A needs to decide whether to forward a packet to another node B in order to have it delivered to node C, it constructs the following proposition – *B is able to reach C within delay requirement $\mathcal{D}$*. Node A also maintains an *evolving graph* [7] to reflect its view of the encounter history. Each link in the graph is based on one verified encounter ticket that A has received. Node A makes observations on the basis of its evolving graph and delay requirement $\mathcal{D}$, and uses the observation results to form its trust opinion towards the proposition stated above.

In the encounter prediction, we develop a *belief* system to evaluate a forwarding candidate's competency based on the Dempster-Shafer theory. The belief assignment will not only reflect node A's belief towards the competency of forwarding candidate B, but also reflect its confidence of the prediction through the measured uncertainty. The formed trust opinion can be regarded as the result of our encounter prediction system, REP. After this process, node A uses the formed trust opinion to decide whether to forward the packet to B.

The contributions of this paper are summarized as follows:

1) We examine both basic and advanced blackhole attacks and the damage they can potentially cause in DTNs.
2) We introduce the notion of encounter tickets in DTNs. Encounter tickets are verifiable contact evidences that guarantee the truthfulness of DTN routing metrics.
3) We design a novel method of interpreting the contact history, in which we link the contact history with the current delivery requirements through observations.
4) We propose an encounter prediction system. Nodes form predicted opinions towards future contacts by utilizing the time information recorded in the encounter tickets.
5) We conduct extensive analysis and real-trace-driven simulations to prove the applicability and advantages of the ticket-based encounter prediction scheme.

II. Related Work

For the related work, we first review the existing DTN routing protocols to show the importance of the truthfulness of the routing metrics. Second, we examine the existing prevention techniques against blackhole attacks in MANETs and show why these techniques fail in DTNs. We also include a brief summary of the major trust management systems as the basis of our encounter prediction system.

A. Metric-based DTN routing protocols

DTNs attempt to route packets via intermittently-connected nodes. This new concept has attracted much research interest. Most of the previous work on DTNs has been based on various assumptions regarding connectivity and the availability of environmental knowledge and control [1], [8], [9], [10]. Some of them even assume that nodes know all future contact information. Since the real mobility trace [2], [11] in the recent experimental DTNs appear to be cyclic to a large extent, several recently-proposed routing protocols in DTNs designed metrics to summarize the information of contact history. These metric-based DTN routing protocols [3], [12] use history to predict the future and are widely applicable. However, all of them assume the truthfulness of the history information and omit the possibility of attacks by providing faked metrics.

B. Attacks with forged metrics in MANETs

The blackhole attack [6], and other attacks with forged metrics, such as wormhole attacks [13], have attracted significant research interest in MANETs. When launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link, known as the wormhole link. The attacker uses the wormhole link to claim and distribute falsified connectivity metrics in an effort to affect routing. The existing countermeasures to these attacks with forged metrics mainly focus on utilizing geometric properties and inherent restrictions of the network. Some of them consider geographical [14] and temporal packet leashes [15]. Others define forbidden substructures [13] in the connectivity graph according to the underlying communication model and graph theory, and detect such substructures to decide whether attackers exist. Since the connectivity or other routing-related metrics comply to certain rules and restrictions in MANETs, these countermeasures are applicable. However, in DTNs, such rules and restrictions of connectivity are invalid due to high mobility and a dynamic topology. Some routing metrics, such as the historical contact probability, are provided by the possible forwarder itself and are hard to verify. This makes the existing countermeasures inapplicable in DTNs.

The idea of provable encounters was also introduced in [16]. However, the scheme in [16] only guarantees that the attacker cannot fabricate acceptable evidence to claim an encounter happened later than the actual encounter time, since hash-chain is used as the verifier. Therefore, this scheme is too restricted in the DTNs, because only last-encounter-based prediction systems such as [5] will benefit from it. In this paper, the prediction metric is not constrained by last-encounter time.

C. Trust management systems

Various frameworks [17], [18] have been designed to model trust networks and have been used as trust management systems. Most trust management systems allow each node to build its own view of other nodes based on its own observations as well as on recommendations from others. Reputation systems, such as CONFIDANT [19] and CORE [20], divide the trust opinion into belief and disbelief. In [21], uncertainty is added and considered to be an important dimension of trust. In DTNs, nodes collect information through direct communication in a distributed manner and form trust opinions based on collected encounter evidence. However, uncertainty is unavoidable as inaccuracy and incompleteness always exist in the collected information. In this paper, we utilize the Dempster-Shafer theory [22] and develop a method for evaluating the competency of a possible forwarder based on the contact history.

III. Underlying Routing Model

The following statements compose the underlying assumptions of our proposal: 1) each node has a fixed buffer size for carrying messages; 2) the packet transmission opportunities are limited in terms of both duration and bandwidth; 3) each node holds a unique ID and a public/private key pair; 4) each packet has a delay requirement $\mathcal{D}$; 5) nodes communicate using radio transmissions. If two nodes reside within the transmission range of each other, then they are considered neighbors; 6) each node holds a public key certificate issued by the PKI.

Our encounter prediction scheme can be directly used in metric-based routing algorithms, such as MaxProp [3] and ProPHET [4]. These routing protocols are designed to increase the throughput and lower the latency under the above assumptions, which are close to the realistic DTN environment. There are typically three stages in metric-based routing: neighbor discovery, packet transmission, and storage management.

Nodes make forwarding decisions solely based on the acquired metrics after neighbor discovery. The estimated delivery likelihood is considered to be the central metric in these routing algorithms. Since nodes do not have a priori knowledge of network connectivity, they can only estimate whether the delivery will succeed in the future based on past experiences. A simple counting method is usually used in metric-based routing algorithms. If two nodes have come in contact many times before, the likelihood of their encounter in the future is considered to be high. Since DTNs usually appear to be repetitive in nature, this estimated delivery likelihood is meaningful when making forwarding decisions. Assume node A has packets to be delivered to node C. Now, if node A meets another node B that has high likelihood of meeting the destination C, then A will replicate and forward the packets to B. Therefore, A's estimated delivery likelihood of B meeting C summarizes A's evaluation of B's competency to send packets to C under the delay requirement $\mathcal{D}$.

Since both buffer size and transmission duration are limited, as the number of replications increases, a packet's forwarding priority decreases, making it more likely to be dropped. To simplify the discussion, we assume that a packet can be replicated and forwarded to, at most, a pre-defined number of forwarders before being deleted from the buffer.

IV. Securing Evidences with Encounter Tickets

Packets in DTNs are opportunistically routed towards the destination, making them robust against simple attacks [23] such as packet dropping attacks. However, in a realistic resource constrained DTN environment, the attacker can greatly reduce the average throughput by providing forged information to attract packets.

A. Attacks with forged information

In the general case, an attacker who forges information aims to cause a severe drop in network throughput. The attacker accomplishes this by falsifying its contact history in an effort to boost its estimated delivery likelihood by reporting its

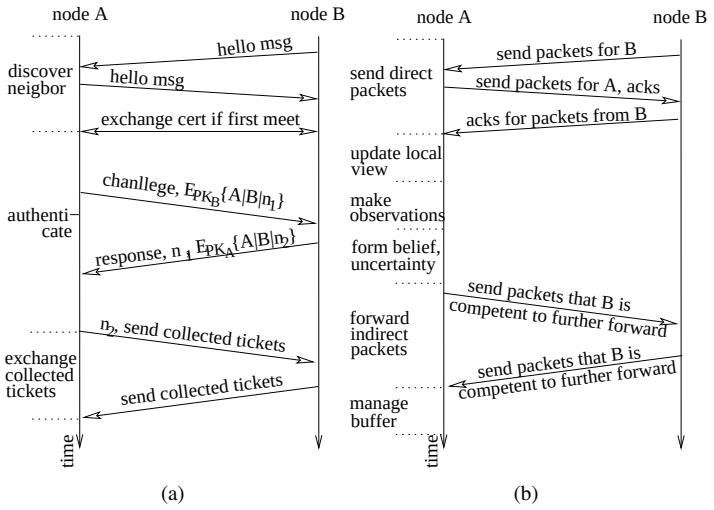


Fig. 2. The process of encounter exchange.

number of previous contacts with some popular destination at the maximum permissible value. This has two effects, both of which cause packets to be drawn towards the attacker instead of its correct destination. A source node encountering the attacker will try to send most of its packets to the attacker, since the attacker's estimated delivery likelihood to popular destinations is high. This creates the belief that the packets have been favorably forwarded. Depending on the forwarding strategy and queueing policy in use, this might hamper future forwarding of the packets and/or lead to premature dropping of the packets. Due to the transitivity, the predicted delivery metrics reported by the attacker will affect the estimated delivery likelihood of other nodes. This will cause a shift in gradient for all destinations towards the attacker as the 'center of gravity'.

An attacker can also target a specific node, say a source or a destination, to launch attacks instead of reducing the network throughput. When isolating a destination, the attacker can report its estimated delivery likelihood towards a particular destination node at the maximum permissible value. By stealing packets intended for a particular node, the attacker can issue an acknowledgement after receiving each packet for its target. This will cause the packet to be removed from the network, thereby greatly reducing its chance of reaching the actual destination. Consequently, the actual destination node will be isolated from the nodes that contact the attacker.

When isolating a source, the attacker needs to contact the source periodically to obtain the list of packets generated by that source, adaptively change its estimated delivery likelihood to attract these packets according to their distinct destinations, and propagate fake acknowledgements to remove these packets. The attacker can also use a distinct fake ID for each contact with the source node to convince the source that its packets have been replicated and forwarded by different nodes.

B. Encounter ticket generation

If we can secure the evidence of each contact, blackhole attackers will not be able to provide a false contact history. The basic idea of our scheme is to generate an unforgeable encounter ticket as the evidence for each contact. When node A moves into node B's transmission range at time t (or vice versa), they will generate an encounter ticket as the evidence for this contact.

Each node is issued a private key (RK) and public key (PK) pair from the certificate authority CA, and a public key certificate signed by the CA's private key. A node also needs to get the destination's public key certificate, either by pre-loading or exchanging, before it generates the packets for the destination.

Frequency control. In the neighbor discovery phase, nodes A and B know each other's node IDs, which are included in the *hello* message. They also need to exchange a public key certificate if it is their first encounter. They authenticate each other based on the public key in the certificate. The process is shown in Fig. 2.

Each node divides the time domain into intervals, and the length of the interval is a pre-defined network parameter. If two nodes are in each other's communication range, only one encounter ticket will be generated in each time interval. After exchanging the above information, the two nodes need to decide upon a timestamp to uniquely identify the time they encountered each other. The timestamp t in the encounter ticket records the index of that interval.

Now the length of the time interval can be adjusted to find a suitable tradeoff between the number of encounter tickets and the accuracy of encounter history. Moreover, this frequency control also reduces the number of encounter tickets that the attacker can get when it follows another node or repeatedly enters and leaves another node's communication range.

Ticket generation. The node with the higher ID generates a new ticket and includes the current time-stamp t, and node IDs A, B in the ticket. The higher ID node then signs it using its private key and sends it to the lower ID node. The lower ID node checks the content of the received raw ticket, attaches its signature if it finds the content to be accurate, sends the signed ticket back to the originator, and stores a copy of the signed ticket. The formal definition is as follows:

Definition 1: **Encounter ticket**: An encounter ticket is a piece of evidence which certifies that nodes A and B encountered at time t. The encounter ticket has the following format:

$$ticket = A, B, t, E_{RK_A}\{H(A|B|t)\}, E_{RK_B}\{H(A|B|t)\}$$

The ticket includes both nodes' signatures to prevent fabrication and modification. Here we use $H(*)$ to denote a hash function, $A|B|t$ to denote the concatenation of A, B, and t, and $E_{RK_A}\{*\}$ to denote the encryption using node A's private key.

Confirmation propagation. For confirmation, when a destination correctly receives a packet, it generates an acknowledgement which bears its signature. Assume A is the source ID, C is the destination ID, and p denotes the packet ID. An acknowledgement has the following format:

$$ack = A, C, p, t, E_{RK_C}\{H(A|C|p|t)\}$$

To enforce the encounter ticket, two nodes exchange packets according to Fig. 2 when they discover each other. Since the encounter tickets and acknowledgements consist of IDs and signatures, they are usually small compared to data packets.

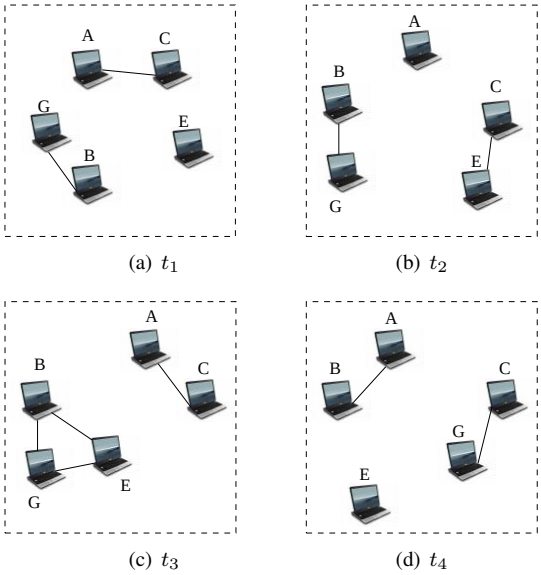


Fig. 3. The evolution of a DTN over time. The indices correspond to the time-stamp of the snapshots.

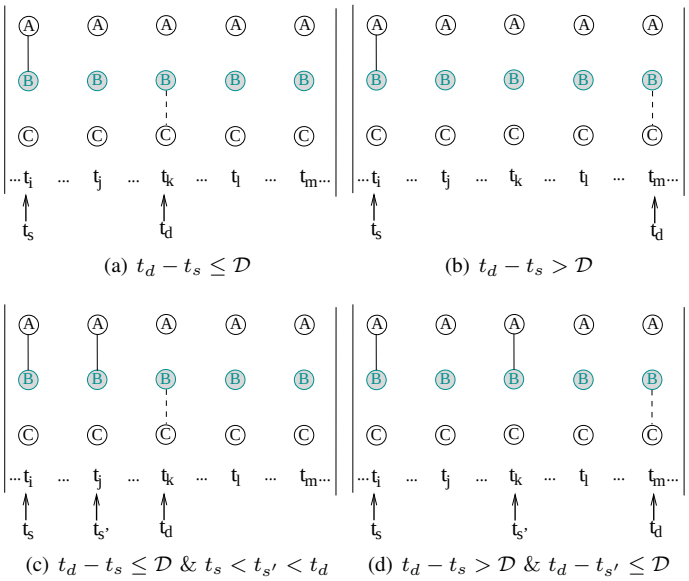
C. Thwarting attacks with forged information

The encounter tickets prevent the attackers from claiming non-existent encounters. Before accepting the encounter ticket between B and C, node A verifies both B and C's signatures in the encounter ticket. Without C's private key, the attacker B cannot forge acceptable encounter tickets to boost its routing metric to attract packets from A. The encryption scheme ensures the truthfulness of the encounter evidence.

The required signature in the acknowledgement prevents the attacker from counterfeiting the acknowledgement after receiving each packet for its target. The attacker can only drop its replication of the packet and cannot cause the packet to be removed from the network. Since nodes authenticate each other before generating the encounter tickets, the attacker cannot use a fake ID for each contact with the source node. Therefore, when isolating a source, the attacker cannot cheat the source node by convincing it that its packets have been replicated and forwarded through different forwarding nodes.

V. Robust History Interpretation

Encounter tickets prevent attackers from giving forged contacts to attract packets. However, the attacker can still boost its estimated delivery likelihood by *tailgating* – an advanced blackhole attack. In this section, we give a detailed description of our ticket-based encounter prediction scheme, which aims at thwarting advanced blackhole attacks in DTNs.



(a) $t_d - t_s \leq \mathcal{D}$ (b) $t_d - t_s > \mathcal{D}$

(c) $t_d - t_s \leq \mathcal{D}$ & $t_s < t_{s'} < t_d$ (d) $t_d - t_s > \mathcal{D}$ & $t_d - t_{s'} \leq \mathcal{D}$

Fig. 4. Four possible situations in observation: (a) no overlap, success, $\alpha \leftarrow \alpha + 1$, β; (b) no overlap, failure α, $\beta \leftarrow \beta + 1$; (c) overlap, one success, $\alpha \leftarrow \alpha + 1$, β; (d) overlap, one failure, one success, $\alpha \leftarrow \alpha + 1$, $\beta \leftarrow \beta + 1$. Solid line denotes a direct connection. Dotted line denotes a possible multi-hop connection. B is the node under observation.

A. Attacks with tailgating mobility pattern

Simply enforcing the encounter tickets and using a ticket-counting mechanism, similar to MaxProp [3], to decide whether or not a node is the qualified forwarder, cannot fully prevent attacks in metric-based routing protocols. Additionally, the simple ticket-counting mechanism abstracts the time information in the encounter tickets, and leaves a convenient way for the attacker to attract packets.

When isolating a destination, the attacker can tailgate the target destination node for a sufficient period of time. Since the target is one specific node, tailgating is easy to implement and the attacker's incurred cost is low since tailgating needs to be carried out only once. The attacker can gather many real encounter tickets during tailgating. This will boost the attacker's estimated delivery likelihood for the target as the estimated delivery likelihood solely depends on the number of previous encounters in current metric-based routing protocols employed in DTNs. Although the frequency control technique can reduce number of tickets an attacker will gather, it cannot prevent the attacker from boosting its routing metric if the attacker tailgate for a long enough period of time. After tailgating, the malicious node simply moves around in the network to attract and drop packets destined for the target destination from other nodes. When isolating a source, the malicious node tailgates the source node instead. By doing so, the malicious node improves its chances of attracting more packets from the source node.

B. History interpretation

To thwart the aforementioned advanced attack scenarios, nodes need to interpret the collected encounter tickets in a way that excludes the attackers' tailgating patterns while reasonably evaluating benign nodes. To accomplish this, after collecting encounter tickets, each node generates a partial view of the contact history represented by an evolving graph. An evolving graph [7] is an indexed sequence of the subgraphs of a given graph where the subgraph at a given index corresponds to the network connectivity at the time interval indicated by the index number. For each encounter ticket a node collects, a link between the corresponding nodes is added to the subgraph with the index number t. Fig. 5 (t_1 to t_4) shows the evolving graph of each of the four snapshots in Fig. 3. Based on a node's current evolving graph, say node A's, the proposition – *node B is able to transmit one packet to node C, given a delay requirement $\mathcal{D}$* – describes the possible forwarder B's competency. Now node A should make observations based on it's accumulated encounter history toward this proposition as the metric to evaluate B's competency.

Node A makes observations based on the evolving graph. Each observation starts at one distinct subgraph in which A and B are directly connected. We assume that the index of that subgraph is t_s. The observation result indicates whether a path over time exists on which the packet can traverse within subgraphs t_s to $t_s + \mathcal{D}$, as shown in Fig. 4. This kind of path is called a *journey*. We use t_d to denote the ending time of a journey. The corresponding variable, α for the existence of such a path in the observation and β for nonexistence, is incremented accordingly.

In our model, there are four possible situations for an observation, as illustrated in Fig. 4. Here we use observation time interval, defined as $[t_s, min\{t_d, t_s + \mathcal{D}\}]$, to represent the time slots that an observation covers. For instance, the observation time interval is $[t_s, t_d]$ in Fig. 4 (a), and the observation time interval is $[t_s, t_s + \mathcal{D}]$ in Fig. 4 (b). In case (a) (Fig. 4 (a)), there is no other direct contact between A and B within $[t_s, t_d]$, and a journey exists from B to destination C within $[t_s, t_d]$. Therefore, we can apply the Dijkstra algorithm and use the earliest arrival time as the cost metric to find the best possible journey. Assuming A has a similar packet with delay requirement $\mathcal{D}$, B would be competent enough to finish the forwarding task in this observation, making the observation result a success. In case (b) (Fig. 4 (b)), since no such journey exists within $[t_s, t_s + \mathcal{D}]$, the observation result is regarded as a failure.

In case (c), the observation starting at t_s has the best possible journey to C ending at t_d. Since $t_d - t_s \leq \mathcal{D}$, the observation result is a success. However, a second direct contact between A and B exists, starting at $t_{s'}$, with $t_s < t_{s'} < t_d$. The observation starting at $t_{s'}$ is also a success since a journey to C within $\mathcal{D}$ exists. Since the observation starting at t_s completely overlaps the time interval of the observation starting at $t_{s'}$, we do not count it as a distinct direct contact. In case (d), since the time intervals of the observations starting at t_s and $t_{s'}$ only partly overlap each other, they should be counted as two separate direct contacts. Therefore, in this case, two observations are made – the result for the one starting at t_s is regarded as a failure and the result for the one starting at t'_s

is regarded as a success. When a node A makes observations of its current contact B, the observation should be defined as below:

Definition 2: **Observation**: Node A makes one observation on node B for each distinct direct contact between A and B in the history. The observation starts at time t_s and ends at time $min\{t_d, t_s + \mathcal{D}\}$. If a journey from B to the destination C exists in the sub-evolving graphs t_s to $t_s + \mathcal{D}$, the observation result is considered to be a success. Otherwise, it is a failure.

VI. Encounter Prediction and Decision Making

The history interpretation results, α (existence) and β (non-existence), cannot be directly used in decision making. For example, assuming A encounters one candidate B with $\alpha = \beta = 5$ and another candidate C with $\alpha = 2$ and $\beta = 1$. A cannot decide which candidate is better without further evaluating the evidence.

A. Measuring competency and evidence sufficiency

Nodes need to measure both competency and evidence sufficiency to make a comprehensive encounter prediction. We follow the Dempster-Shafer theory [22] and develop a belief reasoning process to measure both competency and evidence sufficiency in a unified framework. The Dempster-Shafer theory is a mathematical theory of evidence based on belief functions and plausible reasoning that is used to combine separate pieces of information (evidence) to calculate the probability of an event.

We can formalize the encounter prediction problem in the Dempster-Shafer theory as follows. Remember, node A which has a packet, has a proposition to decide the competency of node B. Let X be the set of all states under A's consideration. The power set, $\mathbb{P}(\mathbb{X})$, is the set of all possible sub-sets of X, including the empty set. Here: $X = \{\{B \text{ is competent}\}, \{B \text{ is incompetent}\}\}$, and $\mathbb{P}(\mathbb{X}) = \{\emptyset, \{B \text{ is competent}\}, \{B \text{ is incompetent}\}, X\}$. According to the Dempster-Shafer theory, the next step is to find a proper mass assignment for $\mathbb{P}(\mathbb{X})$.

We use Bayesian inference as the bridge to connect observation results with the mass assignment. Bayesian inference is a statistical model in which evidence or observations are used to update or to newly infer the probability that a hypothesis is true. The beta distribution, $Beta(\alpha, \beta)$, is used here in the Bayesian inference. The beta distribution is a family of continuous probability distributions defined on $[0, 1]$ differing in the values of their two non-negative shape parameters, α and β. To start with, node A uses prior $Beta(1, 1)$ for B. When a new observation is made, α or β is accordingly incremented. The prior $Beta(\alpha, \beta)$ is then updated. The distribution of $Beta(\alpha, \beta)$ reflects the distribution of the delivery likelihood of node B to destination C under $\mathcal{D}$. Therefore, the mass assignment to $\mathbb{P}(\mathbb{X})$ should be based on $Beta(\alpha, \beta)$

Evidence sufficiency measurement. We first consider how to assign a proper mass for X in $\mathbb{P}(\mathbb{X})$. Here, X includes the scenario that candidate B is either competent or incompetent. Therefore, the mass assigned to the set X in $\mathbb{P}(\mathbb{X})$ should be node A's uncertainty towards the competency of candidate B.

TABLE I
A's belief assignment towards candidate B

Hypothesis	Mass	Belief	Plausibility
Null (neither)	0	0	0
Competent	$b = \frac{\alpha}{(\alpha+\beta)}(1-u)$	b	$b+u$
Incompetent	$d = \frac{\beta}{(\alpha+\beta)}(1-u)$	d	$d+u$
Either	$u = \frac{12 \cdot \alpha \cdot \beta}{(\alpha+\beta)^2 \cdot (\alpha+\beta+1)}$	1	1

We use uncertainty metric u, which is defined in our previous work [21], as the mass assignment towards X. Here, $u \in [0, 1]$. After examining the major statistical metrics of the Beta distribution, we find that the normalized variance satisfies the requirement. Therefore, we define u as follows:

$$u = \frac{12 \cdot \alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)} \tag{1}$$

The variance is multiplied by a constant (12), which makes $u = 1$ when $\alpha = \beta = 1$. The total certainty is $(1 - u)$. This uncertainty reflects the adequacy of the observations.

Competency evaluation. For the certainty part, we should assign mass according to the proportion of supporting evidence in the observation results. Therefore, for the set that $\{B$ is competent$\}$, we should assign following mass b according to standard Bayesian inference:

$$b = E(Beta(\alpha, \beta))(1 - u) = \frac{\alpha}{(\alpha + \beta)}(1 - u) \tag{2}$$

Similarly, the mass d for the set $\{B$ is incompetent$\}$ can be defined. Table I summarizes the belief assignment.

Aging in prediction. When predicting encounters, we want to give the fresh evidence more weight to prevent the attacker from succeeding by being in a non-attacking mode for a period of time and then attacking. Assume a node A starts k observations with node B over a pre-defined period of time. Among these observations, s of them are considered to be successful. A will update α and β at the end of this period by introducing a moving weighted average as follows:

$$\begin{cases} \alpha \leftarrow \mu \cdot \alpha + s \\ \beta \leftarrow \mu \cdot \beta + (k - s) \end{cases} \tag{3}$$

The weight μ is a discount factor for past experiences which serves as the fading mechanism. α_i denotes the total number of recorded successes and β_i denotes the total number of recorded failures after counting the i_{th} time window. $\alpha_0 = \beta_0 = 1$.

B. Decision rules

A node should select and forward the packets to the most competent forwarders with sufficient contact evidences. The forwarding decision rules are critical for curtailing attacks. Fortunately, we can further utilize the Dempster-Shafer theory in making comprehensive decisions.

Shafer's framework allows for belief about propositions to be represented as intervals bounded by two values – belief (or support) and plausibility; belief $\leq$ plausibility. Belief in a hypothesis is constituted by the sum of the masses of all sets enclosed by it. It is the amount of belief that directly

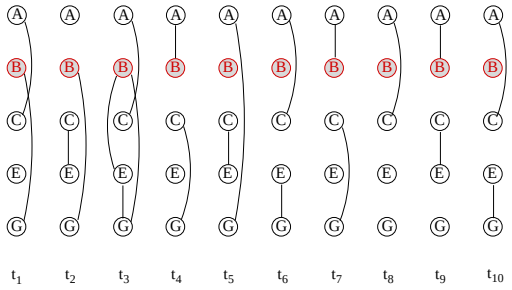


Fig. 5. An evolving graph summarizes the encounter history. Node B is the attacker.

supports a given hypothesis at least in part, forming a lower bound. Plausibility is 1 minus the sum of the masses of all sets whose intersection with the hypothesis is empty. It is an upper bound on the possibility that the hypothesis could possibly happen, i.e. it 'could possibly happen' up to that value, because there is only so much evidence that contradicts that hypothesis. The belief and plausibility of candidate B are both listed accordingly in Table I.

With the lower bound belief and upper bound plausibility, nodes can make more comprehensive decisions, and make forwarding policies according to their own characteristics. An extremely aggressive node would choose the candidate with the highest plausibility as the best candidate. A more conservative node would choose a candidate based on their belief. We can use a characteristic factor c to depict a node's aggressiveness, where $c \in [0, 1]$. Node A should use the metric $(1 - a) \cdot Belief + a \cdot Plausibility$ as the metric to compare the forwarding candidates.

After the pre-selection, we can apply the original metric-based routing protocols to the qualified possible forwarders that are accepted in the pre-selection phase. We substitute the estimated delivery likelihood metric in the metric-based routing protocols with our metric. By doing so, the metric-based routing algorithms are protected from tailgating attackers while reasonably evaluating ordinary nodes' competency.

C. Thwarting advanced attacks

The ticket-based encounter prediction scheme offers protection against advanced attacks in two ways: 1) the definition of observation renders tailgating useless; 2) the decision rules based on the belief and uncertainty guarantee the forwarder's competence as well as the sufficiency of evidence.

An attacker B can tailgate a target node C when B aims to isolate C as a destination. B would be able to get many real encounter tickets before it contacts the possible sources like A. Since each observation starts at a distinct previous contact between A and B, the tickets that B gets from tailgating cannot increase α, which is the number of A's observations with a successful result. Similarly, for the case that B tailgates A to isolate A as a source, B's β increases for the same reasons as discussed above. In our encounter prediction scheme, belief reflects source A's prediction of B's competency based on A's experience of B's competency in similar situations in the contact history, and uncertainty reflects the sufficiency of the experience. To become a favorable forwarder and attract packets, the attacker needs to rapidly move between source and destination to increase A's belief, as well as repeat the journey many times to keep up with the evidence sufficiency requirement. Therefore, the cost of the attack is high and the scope of the attacker is restricted.

As an example, we show the process of node A's forwarding decision. Fig. 5 shows the encounter history from time t_1 to time t_{10}. Assume A generates a packet for G with $\mathcal{D} = 3$ at time t_9 and $c = 1$ in Fig. 5. At time t_9, A meets B. B is an attacker. It tailgates G between t_1 and t_3, and moves to A to attract packets. If we interpret the contact history by simply using a ticket-counting mechanism, B has a good chance of becoming the forwarder since it encounters G three times. However, using our definition of observation to interpret the history, only two observations will be made. One starts at t_7 and this observational result is a failure since no journey exists between B and G in t_8, t_9, and t_{10}. The observation starting at t_4 has a similar situation. Therefore, $\alpha = 1$ and $\beta = 3$. Now, $u = 0.45$ and $b = 0.14$, where $b = 0.28$ for the possible alternative forwarder C. Hence, B cannot attract the packet.

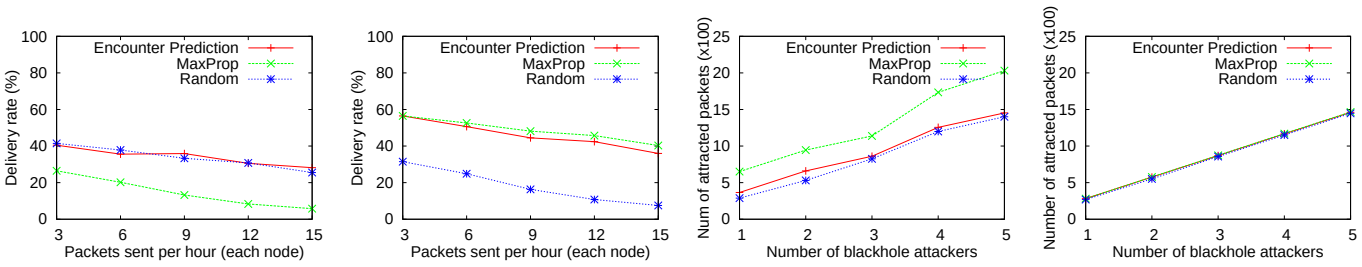
VII. Simulation and Analysis

We conduct simulation studies to evaluate the effectiveness of our ticket-based encounter prediction scheme in preventing blackhole attacks. We compare the effectiveness of our model with two other techniques: MaxProp and random propagation.

A. Simulation setup

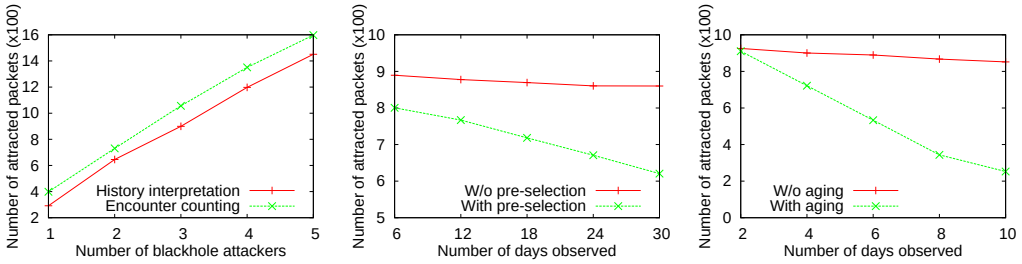
We ran trace-driven simulations with different blackhole attack scenarios. We used the real trace from UMassDieselNet [2] as the basis of honest nodes' mobility patterns. In our simulations, a blackhole attacker is always an intermediate node, while an honest node can be a source, a destination, or an intermediate node. To illustrate the overall network throughput, all honest nodes generate traffic destined for other randomly chosen honest nodes. Since nodes may join or leave the network at any time, some packets may never be delivered even when attackers are not present. Nodes carry a 5 MB buffer in our simulation studies, and packets will be deleted when the buffer is full. In all our simulations, packets are 10 KB in size, the default maximum number of replications is 3, each signature is 128 bits, and the default packet generation rate for each honest node is 12 packets/hr.

The total number of nodes in the network is 33. Of these 33 nodes, we randomly assign blackhole attackers, and at any given time at most 5 such nodes can exist. A blackhole attacker, similar to an honest node, follows the real trace, except for the results presented in Fig. 8 in which we modify the trace to simulate the tailgating mobility pattern. In our simulation studies, we primarily focus on two parameters: (1) the number of packets attracted, and (2) the percentage of packet drops caused by blackhole attackers. The former depicts the efficiency, and the latter measures the extent of damage caused by the blackhole attackers.



(a) Delivery rate without tickets (b) Delivery rate with tickets (c) Packets attracted without tickets (d) Packets attracted with tickets

Fig. 6. The effectiveness of enforcing encounter tickets.



(a) History interpretation (b) Pre-selection (c) Aging in prediction

Fig. 7. Effectiveness of different steps in the encounter prediction.

B. Simulation results

In Figs. 6(a) to 6(d), we compare the situation in which we enforce encounter tickets with the situation in which nodes can claim previous encounters without evidences. Each blackhole attacker adds 100 falsified encounters with random node ID and time-stamp in its encounter list.

In Figs. 6(a) and 6(b), we adjust the packets sent per hour to show the effect of blackhole attacks. We randomly select 3 nodes (10%) to be blackhole attackers. In Fig. 6(a), nodes trust all the previous contact information provided by a possible forwarder. Since there is no verification without enforcing encounter tickets, blackhole attackers can attract most of the packets generated by the nodes which they actually encounter.

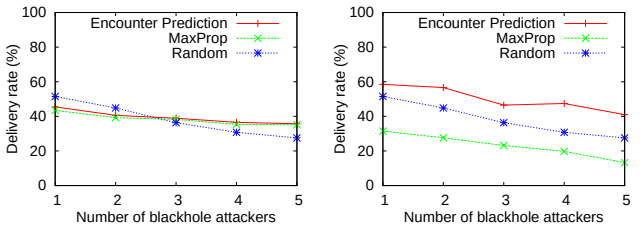
Comparing Figs. 6(a) and 6(b), we can see a significant increase in the delivery rate of the MaxProp algorithm, which shows the extent of damage caused by the blackhole attackers. MaxProp simply uses the number of encounters to determine each node's competence for forwarding a packet. When a node has false contacts, it will be considered to be the most competent node for forwarding to all destinations.

The falsified encounters cannot affect the delivery rate of random propagation. In random propagation, the forwarding decision is made without considering any routing metrics derived from the contact history. Although random propagation is the most robust scheme against blackhole attacks, its delivery rate is significantly lower than the other two schemes when we enforce encounter tickets, as shown in Fig. 6(b).

The requirement of encounter tickets is also important for the encounter prediction scheme, although improvement from Figs. 6(a) to 6(b) seems incremental. This is because the encounter prediction scheme restricts the pattern that one observation will be counted as a success. However, requirement of provable evidence is still necessary since the attackers can fake evidences following certain kinds of patterns. In Figs. 6(c) and 6(d), we adjust the number of blackhole attackers and compare the number of packets attracted by the attackers. Without the encounter tickets, a large number of packets will be attracted and dropped. This further proves the destructiveness of blackhole attacks in the absence of encounter tickets.

In Figs. 8(a) and 8(b), we enforce the encounter tickets and examine the effectiveness of our encounter prediction scheme under different attack scenarios. In Fig. 8(a), the blackhole attackers tailgate one particular source to isolate it during each round of simulation. Under this scenario, the random propagation scheme is the most affected. When an attacker tailgates a source node, its probability of being selected as a competent forwarder increases significantly based on frequent encounters with the source node. However, our encounter prediction and MaxProp schemes are comparatively less affected by this attack scenario since the tickets for encountering the source can neither increase the delivery likelihood metric in MaxProp nor raise the belief in the encounter prediction scheme.

In Fig. 8(b), blackhole attackers aim at isolating random selected destinations, and each accumulates 40 real encounter tickets by tailgating one particular destination before contacting other nodes. MaxProp is the most affected scheme in this scenario, since the real encounter tickets will increase the blackhole attackers' delivery likelihood to the destination when evaluated by other nodes in the DTN. The delivery rate in our encounter prediction scheme is improved by almost 30% on average, since the continuous encounters cannot increase



(a) Delivery rate in isolating-a-src (b) Delivery rate in isolating-a-des

Fig. 8. Delivery rate in different attack scenarios.

the number of successes in the observations, and blackhole attackers cannot attract packets and affect the delivery rate.

Figs. 7(a) through 7(c) show the effectiveness of different steps in our encounter prediction scheme, where the attacker aims to isolate a randomly selected destination. In Fig. 7(a), we assume the blackhole attackers tailgate destination nodes from 06:00:00 to 07:00:00 everyday. When there is only one attacker, it can only attract half of the packets compared to the ticket-counting case. Using our method to interpret the history clearly restricts the blackhole attacker.

In Figs. 7(b) and 7(c), three blackhole attackers tailgate destination nodes only on the first day. We turn the pre-selection decision rule on and off in Fig. 7(b) to show the necessity of evaluating the sufficiency of evidence. Here, an honest node uses its average uncertainty as the threshold. As time passes, the honest nodes accumulate more tickets and consequently the uncertainty threshold becomes more strict. Therefore, the attacker will be filtered out in the pre-selection phase by most of the honest nodes that it encounters. In Fig. 7(c), the aging weight is 0.5. The figure shows that the number of packets attracted by the blackhole attacker sharply decreases when we use an aging mechanism (aging period is one day in this simulation).

Our simulation results can be summarized as follows: 1) Without mandating encounter tickets, the blackhole attackers can greatly decrease the delivery rate in DTNs; 2) The number of packets attracted and dropped by the attackers is significantly lower when using the ticket-based encounter prediction scheme, compared to MaxProp or random propagation; 3) Our encounter prediction scheme restricts the effect of tailgating in advanced attacks, tailgating cannot bring more advantages to the attacker than the random movement; 4) History interpretation, competency evaluation, evidence sufficiency checking, and aging are effective steps in thwarting advanced attacks.

VIII. Conclusion

Several DTN routing algorithms adopt the estimated delivery likelihood as the primary routing metric. With this comes the risk of malicious nodes providing forged metrics to attract packets for launching attacks. In this paper, we propose an encounter ticket scheme to secure the evidence of contacts, upon which nodes base their computed belief and uncertainty towards the competence of each potential forwarding node. Then, using the encounter prediction scheme proposed in this paper consisting of history interpretation, competency evaluation, evidence sufficiency checking, and aging, nodes make forwarding decisions that prevent attackers from boosting their routing metrics. In the future, we plan to investigate collusion between malicious nodes. Two attackers can generate many encounter tickets with false future time-stamps. It is similar to the false praise attack in the trust system.

Acknowledgments

This work was supported in part by NSF grants CNS 0422762, CNS 0434533, CNS 0531410, and CNS 0626240.

References

[1] S. Jain, K. Fall, and R. Patra. Routing in a delay tolerant network. In *Proc. of ACM SIGCOMM*, 2004.
[2] A. Balasubramanianm, B. Levine, and A. Venkataramani. DTN routing as a resource allocation problem. In *Proc. of ACM SIGCOMM*, 2007.
[3] J. Burgess, B. Gallagher, D. Jensen, and B. Levine. Maxprop: Routing for vehicle-based disruption-tolerant networks. In *Proc. of IEEE INFOCOM*, 2006.
[4] A. Lindgren and A. Doria. Probabilistic Routing Protocol for Intermittently Connected Networks. *draft-lindgren-dtnrg-prophet-03*, 2007.
[5] H. Dubois-Ferriere, M. Grossglauser, and M. Vetterli. Age matters: Efficient route discovery in mobile ad hoc networks using encounter ages. In *Proc. of ACM MobiHoc*, 2003.
[6] Y. Hu and A. Perrig. A survey of secure wireless ad hoc routing. In *Proc. of IEEE Security and Privacy*, 2004.
[7] A. Ferreira. Building a reference combinatorial model for MANETs. *IEEE Network*, 18(5):24–29, 2007.
[8] S. Merugu, M. Ammar, and E. Zegura. Space-time routing in wireless networks with predictable mobility. In *Technical Report GIT-CC-04-07, College of Computing, Georgia Institute of Technology*, 2004.
[9] A. Pentland, R. Fletcher, and A. Hasson. Daknet: Rethinking connectivity in developing nations. *IEEE Computer*, 37(1):78–83, 2004.
[10] B. Burns, O. Brock, and B. Levine. MORA routing and capacity building in disruption-tolerant networks. *Elsevier Ad hoc Networks Journal*, 6(4):600–620, June 2008.
[11] L. Song and D. Kotz. Evaluating opportunistic routing protocols with large realistic contact traces. In *Proc. of ACM MobiCom Workshop on Challenged Networks (CHANTS)*, 2007.
[12] T. Spyropoulos, K. Psounis, and C. S. Raghavendra. Spray and focus: Efficient mobility-assisted routing for heterogeneous and correlated mobility. In *Proc. of IEEE PERCOM*, 2007.
[13] R. Maheshwari, J. Gao, and S. R. Das. Detecting wormhole attacks in wireless networks using connectivity information. In *Proc. of IEEE INFOCOM*, 2007.
[14] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proc. of ACM MobiCom*, 2002.
[15] J. Eriksson, S. Krishnamurthy, and M. Faloutsos. Truelink: A practical countermeasure to the wormhole attack. In *Proc. of IEEE ICNP*, 2006.
[16] S. Capkun, L. Buttyan, and J. Hubaux. Sector: Secure tracking of node encounters in multi-hop wireless networks. In *Proc. of ACM SASN*, 2003.
[17] Y. Sun, Z. Han, W. Yu, and K. Liu. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In *Proc. of IEEE INFOCOM*, 2006.
[18] M. Carbone, M. Nielsen, and V. Sassone. A formal model for trust in dynamic networks. In *BRICS Report RS-03-4*, 2003.
[19] S. Buchegger and J. Boudec. Performance analysis of the confidant protocol. In *Proc. of ACM MobiHoc*, pages 226–236, 2002.
[20] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Communications and Multimedia Security*, pages 107–121, 2002.
[21] F. Li and J. Wu. Mobility reduces uncertainty in MANETs. In *Proc. of IEEE INFOCOM*, 2007.
[22] G. Shafer. *A Mathematical Theory of Evidence*. Princeton University Press, 1976.
[23] J. Burgess, G. Bissias, M. Corner, and B. Levine. Surviving attacks on disruption-tolerant networks without authentication. In *Proc. of ACM MobiHoc*, 2007.