Mobi-Herald: Alert Propagation in Mobile Ad Hoc Networks

Wenbo He Ying Huang Klara Nahrstedt
Department of Computer Science
201 N. Goodwin Avenue
Urbana, IL 61801-2302

Whay C. Lee
Motorola Labs
111 Locke Drive
Marlborough, MA 01752

***Abstract*— Intrusion/misbehavior detection and response are two important components for defending against various attacks in mobile ad hoc networks. Unfortunately, there is a gap between local intrusion/misbehavior detection and network-wide response in such networks. To bridge this gap, alert propagation, aiming to spread alert messages to the whole network upon detection of malicious/abnormal activity, is a viable solution but has been overlooked. Epidemic routing schemes are available to propagate messages to the entire network. However, alert propagation cannot simply rely on epidemic routing schemes only, because these schemes can be utilized by malicious nodes (slanderers) to defame other network nodes to issue *DoS* attacks. In this paper, we present a novel protocol for alert propagation, called *Mobi-Herald*. To achieve high coverage of message delivery, we design a novel mobility-assisted epidemic routing scheme to propagate alert messages efficiently. To defend against slander attack, our *Mobi-Herald* alert propagation scheme adopts threshold-based verification against collusive slanderers. To ensure transmission efficiency, we use control parameter *times-to-send (TTS)* to limit unnecessary transmissions. We evaluate the *Mobi-Herald* alert propagation protocol through both theoretical analysis and simulation. We conclude that *Mobi-Herald* achieves excellent coverage of message delivery with small message overhead and reasonable alert propagation delay.**

I. Introduction

The need for pervasive and ubiquitous communications makes mobile wireless ad hoc networks (MANETs) increasingly attractive. However, due to the shared-medium nature of wireless links, an adversary can easily intercept legitimate traffic, tamper with original traffic, or inject superfluous traffic in a wireless ad hoc network to degrade the performance of the network. To deal with such malicious attacks in MANETs, attack detection schemes [1], [2], [3] have been proposed. Usually only surrounding nodes of a malicious node are likely to detect its intrusion/misbehavior. As long as the surrounding nodes of an attacker become aware of intrusion/misbehavior of the attacker, they can adapt routing behavior to prevent/nullify future attacks. However, an attacker (or a malicious node) may move arbitrarily, and it can be a neighbor of any friendly node in a mobile ad hoc network. Therefore, to trigger network-wide reaction against malicious attacks, almost all network nodes need to be aware of the malicious node. Alert propagation schemes are required to fill the gap between local "intrusion/misbehavior detection" and network-wide "response".

It is challenging to design an efficient, reliable and robust alert propagation scheme in MANETs. *First*, the alert propagation scheme must be efficient in terms of aggregate bandwidth consumption. *Second*, the alert propagation must be reliable so that each alert message should reach almost all network nodes, even when a network is subjected to failures, packet loss, and intermittent partition. *Third*, an alert propagation scheme must be able to defend against a *slander attack*, which is an attack to defame a friendly node in the network. Otherwise, the alert propagation scheme can be utilized by malicious nodes to defame friendly nodes and cause them to be isolated by others in the network. This is essentially a type of denial-of-service (*DoS*) attack. *Fourth*, the alert propagation should be robust under dynamic environments. In a wireless mobile ad hoc network environment, topology and neighborhood information are dynamic. Both malicious nodes and friendly nodes move continually, hence the maintenance of frequently changing topology and neighborhood information incurs a large overhead.

Epidemic routing schemes are available to propagate messages to an entire network. Previous effort on epidemic routing protocols focuses on two classes: (1) flooding [4], [5] and its variations [6], [7], [8], [9]; and (2) mobility-assisted epidemic routing for intermittently connected networks [10], [11]. Flooding-based epidemic routing protocols require relatively high node density to ensure reliability of message delivery (so that a message can be delivered to the whole network). Existing mobility-assisted epidemic routing protocols, which are typically designed for sparse networks or frequently partitioned networks, offer reliable message delivery. However, these epidemic routing schemes alone are unable to meet the requirements of alert propagation, including transmission efficiency, reliability, defense against slander attacks, and robustness.

In this paper, we first present a novel mobility-assisted epidemic routing scheme. Then, we generalize it for alert propagation in mobile ad hoc networks by suppressing illegitimate alert messages generated by *slanderers*. To the best of our knowledge, this paper is the first on alert propagation in mobile ad hoc networks. There are three components involved in our alert propagation protocol: *mobility-assisted epidemic routing*, *threshold-based verification* and *alert propagation management*. *Mobility-assisted epidemic routing* is the underlying component which aims to disseminate messages to all network nodes efficiently. In our *mobility-assisted epidemic routing* scheme, a herald is defined as a mobile node which actively participates in message dissemination. A mobile herald periodically transmits a message to be propagated in its neighborhood. With mobility of the herald and its

periodical retransmissions, a message can be disseminated to the whole network efficiently. In the *mobility-assisted epidemic routing* scheme, a *times-to-send (TTS)* field is included in the header of a message. In each period, when a mobile herald retransmits a message, *TTS* value is reduced by one. When *TTS* reaches zero, a node stops forwarding the message. Hence, the alert propagation procedure on the herald node is terminated. *Threshold-based verification* is employed to defend against *slander attacks*. A friendly node must have received enough alert messages regarding an alert, before it can trust the alert message and participate in further alert propagation. *Alert propagation management* is designed to control termination of a periodic alert propagation procedure by determining the parameter *TTS*, so that an alert message can be disseminated with a high probability to all network nodes with small message overhead. Intuitively, a larger *TTS* implies a larger number of retransmissions, and thus it is likely that the message will reach more nodes. However, more retransmissions incur more message overhead. To reduce message overhead, we use the minimum *TTS* that ensures almost all nodes can finally receive the alert message in alert propagation.

The rest of this paper is organized as follows: Section II reviews related work and introduces the background of this paper. Section III describes our proposed architecture of *Mobi-Herald* alert propagation and sets the context of our work. Section IV introduces the *mobility-assisted epidemic routing* scheme. Section V shows the threshold-based verification used to defend against malicious *slander attacks* in the system. Section VI describes how we can determine a minimum *TTS* for alert propagation. Section VII evaluates performance of the *Mobi-Herald* protocol based on simulation results. We conclude the paper in Section VIII.

II. Related Work

In this section, we first summarize the two categories of existing epidemic routing protocols: flooding-based protocols, and mobility-assisted epidemic routing protocols. Then we review some existing work supporting alert propagation.

A. Epidemic Routing Schemes

1) Flooding and Its Variations: Several variations of the flooding protocol are available. Due to message redundancy, flooding consumes scarce bandwidth resources in a wireless ad hoc network, leads to heavy contention, and causes packet loss over wireless links. To reduce message redundancy, several schemes have been proposed: In probabilistic or counter-based schemes [6], [12], [13], nodes rebroadcast a message with probability p. A predetermined p is used in [6]. However, in sparse networks the probabilistic scheme with a predetermined p cannot guarantee that all nodes in the network can receive a broadcasting message. The flooding schemes usually trade off reliability for efficiency in terms of communication overhead. Mistral [9] introduces a scheme to achieve balance between efficiency and reliability. Mistral uses probabilistic flooding as a base line, but compensates for dropped messages by periodically broadcasting compensation messages, each of which consists of a set of dropped messages. In neighborhood knowledge based schemes, nodes update their neighbor list by periodically sending "HELLO" messages. Self pruning protocol [15] requires that each node have knowledge of its one-hop neighbors. A sender of a broadcast message includes its neighbor list in the header of the message. Upon receiving the message, a node compares its neighbor list to the sender's neighbor list. If the node can reach additional nodes by rebroadcasting the message, it rebroadcasts the message; otherwise the message is dropped. Scalable Broadcast Algorithm (SBA) [7] and Double Covered Broadcast (DCB) [8] both require two-hop neighbor knowledge, but use different methods to select a set of nodes to rebroadcast a message. In MANETs, nodes may move constantly and neighborhood information changes very frequently. In this case, it is very expensive to maintain neighbor lists.

2) Mobility-Assisted Epidemic Routing: The simplest of the mobility-assisted routing schemes is to let a source node deliver a message to its destination node only when the nodes are within transmission range of each other. Such a scheme has minimal communication overhead. However, delay of such scheme can be very large. A "two-hop relay" scheme has been proposed in [16], where a source node randomly chooses a relay node within its one hop distance to forward a message, so that the relay node can send the message to the destination node when the two nodes come within transmission range of each other. The message path is at most two hops long. Although the "two-hop relay" scheme achieves a $\Theta(1)$ capacity per node, a long message delivery delay is expected. Along this direction, various trade-offs between capacity and delay have been explored [17], [18], [19], [20].

Recently, mobility-assisted routing schemes have attracted much research effort in delay tolerant networks (DTNs), where mobility is a necessary component of the routing functionality. In DTNs, mobility is utilized to reduce the number of transmissions to deliver a message from the source to the destination. A comprehensive overview of mobility-assisted routing schemes is provided in [21]. Here we briefly discuss a few representative protocols on mobility-assisted epidemic routing schemes. For example, epidemic routing is employed to achieve end-to-end message delivery in intermittently connected networks [10] and [11]. Using epidemic routing to achieve end-to-end delivery is able to reduce the end-to-end delay significantly, but it consumes more network resources (e.g. bandwidth and storage), since all nodes in the network may serve as relay nodes for the message. For bandwidth efficiency, a *summary vector* [10] is used to indicate whether or not a given message is in the local buffer of a certain node. When two nodes come into the communication range of each other, they exchange their *summary vectors*. Hence, each node knows which messages it has not yet received. Then the two nodes exchange messages accordingly. The protocol based on *summary vectors* is designed for partially connected networks, which are usually sparse networks. A reasonably dense mobile ad hoc network can be overloaded when many nodes exchange pairwise *summary vectors*.

B. Alert Propagation

There are several systems supporting alert propagation in peer-to-peer (P2P) networks. "ContagAlert" [22] is based on contagion theory. Each node in a P2P network has several neighboring peers. If its number of alerted neighbors exceeds a certain threshold, the node becomes alerted and notifies its neighbors. "Vigilante" [23] system adopts self-certifying alerts to guard against Internet worms and utilizes a small dedicated set of nodes for alert propagation. However, these techniques do not apply in the context of mobile ad hoc networks because the implicit assumptions of these systems are not realistic in mobile ad hoc networks: first, the network has unlimited bandwidth; second, the nodes are static. In this paper, our goal is to design an alert propagation protocol with minimal bandwidth consumption in mobile ad hoc networks, and at the same time suppress the malicious alert messages generated by adversaries.

III. Background and *Mobi-Herald* Alert Propagation Framework

A. Attack Model

Mobile ad hoc wireless networks are vulnerable to various attacks by malicious nodes due to their open multiple access medium. These malicious nodes (or attackers) could degrade network performance and even deny legitimate nodes of service. We consider two types of active attacks. In the first type, an adversary may inject illegal traffic, as well as intercept, interfere, or tamper legitimate traffic. Attacks of this type are caused by the misbehavior of attackers, and are referred to as *misbehavior attacks*. The second type of attacks is the *slander attack*, where an attacker defames a friendly network node by disseminating illegitimate alert messages. While other network nodes receive such illegitimate alert messages, they distrust the victim friendly nodes. In this way, a malicious node may bring down a portion of the network nodes, and the network may be partitioned. We define a *slanderer* as an adversary that initiates an illegitimate alert message to defame a friendly node and starts to propagate the illegitimate alert message.

The shared-medium nature of wireless links facilitates "neighborhood watch" among peer wireless nodes. The design of abnormality detection schemes is beyond the scope of this paper, and has been discussed in [1], [2], [3], etc. Figure 1 illustrates that the ability of a node to detect abnormality depends on its location. If a node is located in the intersection of two circles in Figure 1, it is able to detect the abnormality of the malicious node.

If all neighbors around a malicious node are aware of it, the network is immune to the attacks issued by the malicious node. However, in an arbitrary mobility pattern, a malicious node can be a neighbor of an arbitrary network node. Therefore, upon detecting an intrusion by a malicious node, the detectors need to alert almost all other network nodes such that the network nodes could adapt their routing behavior to prevent/nullify future attacks by the malicious node. However, in the alert propagation procedure, we must suppress the illegitimate alert message forged by *slanderers*. If we simply use an epidemic routing algorithm to propagate the alert message, the performance loss can be doubled under the slander attack. First, friendly nodes waste bandwidth and energy to spread the illegitimate alert message. Second, if all other nodes believe the illegitimate alert message, the whole network will try to isolate the victim node identified in the illegitimate alert message. It is even worse if multiple *slanderers* collaborate to defame a set of friendly nodes. Such a *slander attack* is a type of *denial-of-service (DoS)* attack.

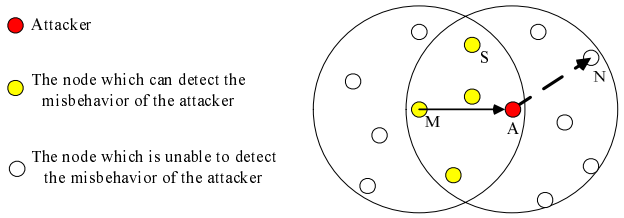


Fig. 1. Node M is the upstream neighbor of an attacker A, and node N is the downstream node of the attacker. If a node, say S, is within the transmission range of both A and M, then the node is able to detect A's misbehavior, since S can overhear the message forwarded by M and the message relayed by A. If the attacker A tampers or maliciously drops the original packet (data or routing message), then S can sense it. If the attacker A detours the packet by forwarding the packet to a node other than N, S can detect it as well.

B. Design Goals

In this paper, we address the following design concerns:

(1) Efficiency: We desire to distribute messages through mobile ad hoc networks by consuming minimum aggregated resources, such as network bandwidth. Here, we use the total number of transmissions for alert message delivery as a metric for the aggregated resource consumption.

(2) Reliability: We measure the reliability of alert propagation with the coverage of alert message delivery. The coverage means the percentage of network nodes which have received (or confirmed) the alert message. The alert propagation must balance the conflicting goals of maximizing coverage of alert message delivery and minimizing the aggregated resource consumption.

(3) Suppression of Illegitimate Alert Messages: Due to the presence of *slander attacks*, alert propagation must be able to suppress (or impair) illegitimate alert messages generated by *slanderers*. We desire a high suppression rate of illegitimate alert messages.

(4) End-to-end Alert Message Propagation Delay: End-to-end alert message propagation delay is measured by the time used for alert propagation. In alert propagation, we usually do not require immediate delivery of an alert message to all the network nodes. However, the delay should not be too large. As long as network nodes are aware of the alert about the malicious node before the malicious node moves to their neighborhood, the network nodes can establish fruitful defense.

C. Assumptions

To make our design fit in a wide range of mobile ad hoc network systems, our *Mobi-Herald* protocol does not require network nodes to maintain neighborhood information. To set up context of this paper, we make assumptions as follows:

(1) *Agility*: Each network node has a reasonable likelihood of moving around. Network nodes (e.g. pedestrians

and vehicles) may move at various speeds and may halt for a while from time to time. Hence, *agility* assumption is naturally satisfied in mobile ad hoc networks.

(2) *Autonomy*: Each node has independent control over its movement and the route of a mobile node is determined by the node itself. Other nodes cannot interrupt the movement or predict the trajectory of a mobile node.

D. System Architecture

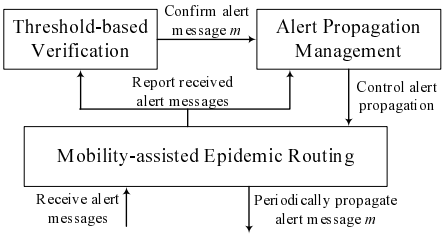


Fig. 2. System architecture of *Mobi-Herald* alert propagation

Figure 2 depicts the system architecture of *Mobi-Herald* alert propagation protocol. The underlying component for alert message distribution is the *epidemic routing* component, which utilizes node mobility to propagate alert messages efficiently. *Threshold-based verification* component helps to suppress the illegitimate alert messages generated by *slanderers*. Before a node confirms the authenticity of the alert message, it does not actively propagate the alert message. Assuming k as the maximum number of collusive *slanders*, the *threshold-based verification* confirms authenticity of the alert message only when the node has received more than k copies of the message from different nodes. Note that it is crucial to correctly estimate and anticipate parameter k in a mobile ad hoc network, since the selection of k affects end-to-end delay, message overhead, reliability and ability to suppress illegitimate alert messages of alert propagation. Fortunately, k does not need to be very large for two reasons: *First*, the number adversaries which steal *IDs* and authentication keys cannot be very large. *Second*, under the context of our alert propagation scheme, even if the number of collusive *slanderers* exceeds k, the *slanderers* need to consume much larger resources to issue *slander attacks* if we select a reasonable value for k (details will be explained in Section V). In a mobile ad hoc network, an adversary usually has limited resources (bandwidth and battery), it is not wise for an adversary to sacrifice much larger resources than a friendly node to issue an attack.

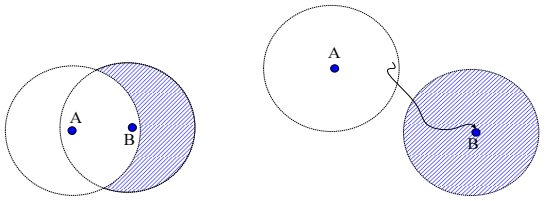
After the threshold-based verification confirms the authenticity of the alert message, the node becomes a "mobile herald", and actively participates in the alert propagation. *Alert propagation management* component controls when the alert propagation procedure should stop by determining a value of *Times-to-send (TTS)*. The parameter *TTS* tells epidemic routing component how many rounds a node forwards the alert message before the alert propagation stops. It is desired that if all network nodes have confirmed the authenticity of an alert, the alert propagation procedure can be terminated and release the network resources. Otherwise, tremendous bandwidth will be consumed in vain. Section VI suggests algorithms to determine a proper *TTS* value in alert propagation.

IV. *Mobility-assisted* Epidemic Routing

In this section, we will introduce a mobility-assisted epidemic routing scheme.

A. Advantages of Mobility-assisted Epidemic Routing

Our experiments show that in a reasonably dense network, it is very likely that flooding protocol (without utilizing mobility) only delivers the message to a small portion of network node. This is because in a snapshot view of the network, even though the network has reasonable density, node mobility frequently causes uneven node distribution, and results in network partition. Mobility-assisted routing schemes allow message carriers to forward the message from different locations, which is equivalent to "multi-source flooding". Hence, mobility-assisted routing schemes can achieve large coverage of message delivery.



(a) Coverage of B's transmission without utilizing mobility

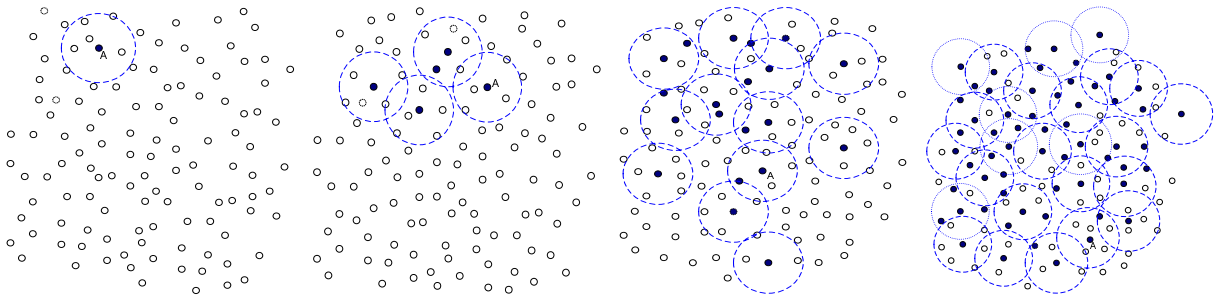
(b) Coverage of B's transmission in mobility-assisted protocols

Fig. 3. Mobility helps to disseminate message efficiently: When node A spreads a message, node B hears it. Without utilizing mobility in (a), B forwards the message to its neighbors upon reception of the message. The additional coverage of B's transmission is shown as the shaded area in (a). In (b), after B receives the message, it moves from the original location to a new location, and forwards the message in the new location, then the message coverage of B's transmission is the shaded area in (b).

Another advantage of mobility-assisted schemes is that message retransmissions may achieve larger coverage than those in static case (see Figure 3). Hence, re-transmissions in mobility-assisted epidemic routing protocols can be more efficient. Based on such observation, we design a mobility-assisted epidemic routing protocol, and then build the alert propagation protocol on top of it. In *mobility-assisted* epidemic routing scheme, an alert message carrier, also called a *herald*, forwards the message periodically.

B. Overview of Mobility-assisted Epidemic Routing

Without considering *slander attacks*, upon receiving a message, a network node becomes a mobile herald and begins forwarding the message periodically. Each period between retransmissions of a message has a duration T. Figure 4 demonstrates the *mobility-assisted* epidemic routing protocol. Initially, a node carries a message, and it serves as a *mobile herald*. At $t = t_0$, the node (dark node in Figure 4) broadcasts the message to other 4 nodes in its neighborhood as shown in Figure 4(a). Thus, t_0 marks the time when the message propagation begins. A node is alerted if it has received at least one copy of the alert message. Immediately after t_0, 5 nodes have



(a) At time $t = t_0$ (b) At time $t = t_0 + T$ (c) At time $t = t_0 + 2T$ (d) At time $t = t_0 + 3T$

Fig. 4. Illustration of *mobility-assisted* epidemic routing

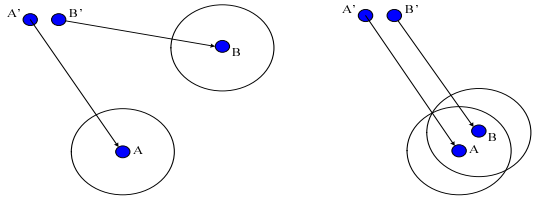
been alerted, and become *mobile heralds*. During time $[t_0, t_0+T)$, the 5 nodes (dark nodes) carrying the message move to new locations, and propagate the alert in their respective neighborhoods in (Figure 4(b)). Note that one of the 5 nodes suppressed transmission in this period (we describe the suppress scheme in Section IV-C). In such a way, more and more nodes become alerted and serve as *mobile heralds* (dark nodes) to further propagate the message (Figure 4(c)). With node mobility, a node encounters different neighboring nodes from time to time. In this way, *mobile heralds* (the nodes which carry a message) bring the message to more and more nodes, and more and more nodes become *mobile heralds* to accelerate the message propagation. Therefore, after a few steps (e.g. by time $t = t_0+3T$ in Figure 4(d)), almost all the network nodes have received the message, and thus become alerted.

C. Suppression of Transmissions

For the sake of efficiency in terms of message overhead, a node should suppress transmission if necessary. Assuming two nodes carry a message in Figure 5, if the two nodes move to different locations, such that their transmission areas do not overlap (in Figure 5(a)), then they can retransmit their copies of the message without redundant coverage. However, if the two nodes are close enough to each other, such that one of the retransmissions by these two nodes does not yield much additional coverage, as shown in Figure 5(b). In this case, one of the retransmissions could be suppressed to reduce message overhead. In our *mobility-assisted epidemic routing* protocol, if a node hears the transmission of an alert message within a short period from its neighborhood, the node suppresses the transmission of the message.

Figure 6 demonstrates message retransmission schedule at each mobile herald. In order to design efficient suppression scheme, retransmissions of a message should occur within a small time slot Δ in each local time period. Assuming that a node schedules the transmission of a message at time t, if the node hears the transmission between $[t-\Delta-\tau_{max}, t)$, where τ_{max} is the upper bound of clock drift between two nodes, then it suppresses the transmission. Upon receiving a message initiated at t_0, each node retransmits the message at most once during local time $[t_0 + \delta T - \Delta, t_0 + \delta T]$, where $\delta = 1, 2, 3, \cdots$ and $\Delta \ll T$.

Note, although we use the same T for all message carriers to retransmit, the nodes are not required to be



(a) Carriers are far apart from each other (b) Carriers are close to each other

Fig. 5. Two message carriers move from their original locations A' and B' to current locations A and B. If they are apart from each other in (a), then the covered area by two transmissions are not overlapped, thus two transmissions yield the maximum coverage. If they are close to each other, the covered area by two transmissions are reduced, hence one of the transmissions should be suppressed for efficiency purpose.

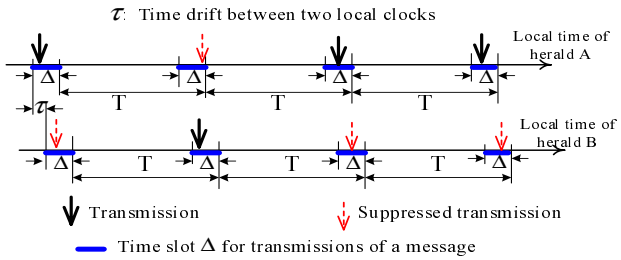


Fig. 6. Retransmission schedule of two neighboring heralds

synchronized as long as the value of Δ is not too small. Actually, the intrinsic imperfect clock synchronization can help to avoid concurrent transmission in a neighborhood. Otherwise, randomness is utilized to achieve this goal.

D. Parameter T

In the *mobility-assisted* protocol, nodes carrying a message periodically broadcast the message to its neighbors. Intuitively, if the period T is large, then the delay of the message delivery is very large. However, if T is too small, the neighbors of a node do not change too much from time $t_0+(\delta-1)T$ to $t_0+\delta T$, hence the transmission at $t_0+\delta T$ only makes the message reach a small number of nodes which have not received message before. We desire that the coverage of two continuous transmissions by a mobile herald has no overlap (in Figure 7). Therefore, we have $T = \frac{2r}{v_{avg}}$, where r is the transmission range, and v_{avg} is the average velocity that a network node moves.

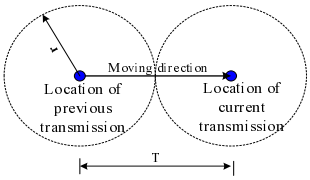


Fig. 7. Determination of T

E. Algorithm

A *times-to-send (TTS)* field is included in an alert message. When a node initiates an alert message m, it attaches a positive *times-to-send (TTS)* value to the message m and serves as a mobile herald of m at time t_0. With the message propagation procedure going on, more and more network nodes become heralds which actively propagate message m to their neighbors. These mobile heralds follow *Algorithm 1* for epidemic routing in each period. At time $t_0 + \delta T$ $(\delta = 1, 2, 3, \cdots)$, if *TTS* is larger than zero, the mobile heralds reduce the *TTS* by one and retransmit message m to their neighbors unless a node hears someone else has transmitted the message around time $t_0 + \delta T$ in its neighborhood.

A *TTS* value indicates the maximum number of transmissions that a mobile herald will broadcast an alert message. For example, the herald node A in Figure 4 transmits its message 4 times, if we set *TTS=4*. It is an important design issue to determine *TTS* in a mobile ad hoc network so that almost all nodes can receive a message before *TTS* of the message reaches zero. We will discuss this issue in Section VI.

Algorithm 1:
Mobility-assisted Epidemic Routing for a Message m

While ($m.TTS > 0$) {
  Wait for T time slot.
  Set $m.TTS = m.TTS - 1$.
  If the node heard the transmission from a neighbor in $[t_0 + \delta T - \Delta, t_0 + \delta T)$ time slot, where $\Delta \ll T$, then
    Suppress the transmission;
  Else
    Transmit the message.
}

V. Threshold-based Verification

Without considering *slander attacks*, whenever a node receives a message, the node becomes a mobile herald to actively propagate the message. However, under the presence of collusive *slander attacks*, a network node cannot tell whether the received alert message is illegitimate and generated by *slanderer* nodes. To suppress the propagation of illegitimate alert messages, we employ *threshold-based verification* to fight against collusive slander attacks. We assume that there are at most k collusive slanderers in a network, since malicious nodes cannot compromise arbitrarily large fraction of the network. A friendly node confirms the authenticity of an alert message only when it has received more than k alert messages from different nodes[1]. Moreover, the friendly node participates in the alert message propagation (or serves as a mobile herald) only after it confirms the authenticity of the alert message. In the *threshold-based verification*, a threshold value $Q = k+1$ is able to defend against at most k collusive attackers in the system. Note that in the epidemic routing scenario, where we do not care about slanderers in the system, we set $k = 0$[2]. For individual *slander attacks*, we set $k = 1$.

A. State Transition in Alert Propagation

We use three states to model a network node in the alert propagation. Figure V-A illustrates the state transition diagram of a node in *Mobi-Herald* alert propagation scheme. Originally, all nodes are in "unaware" state until the malicious behavior is detected by at least one detector. Each detector confirms the alert regarding the malicious behavior directly, and transits to "confirmed" state. For a node which does not detect the malicious behavior, the node switches to "alerted" state upon reception of the first alert message. In the "alerted" state, a node does not broadcast the alert message, since the node cannot tell whether or not the alert is generated by malicious *slanderers*. When a node has collected at least Q messages, it confirms that the alert message is legitimate. Hence, only if a node is in the "confirmed" state, it serves as mobile herald and broadcasts the alert message periodically.

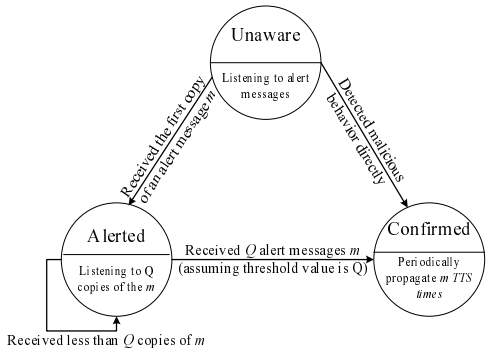


Fig. 8. State transition diagram of a node for an alert message m

For a threshold Q, the epidemic routing component of a network node does not suppress the transmission until it hears Q transmissions in a single time slot.

B. Selection of k

k is an important parameter in *threshold-based verification*. Let us define $\tilde{k}$ as the actual number of collusive *slanderers*. It is ideal that we choose $k = \tilde{k}$, but that is not always possible in practice. However, it is not necessary to know $\tilde{k}$, and have k match $\tilde{k}$ exactly. Usually, a mobile adversary has limited resources, hence a wise *slanderer* desires to issue *slander attack* without consuming too much of its own resources. We can select k so that each *slanderer* must consume much more resources than a

[1]Alert messages are attached with signatures in order to prevent fake ID attacks.

[2]Note that there exist misbehavior attacks other than slander attacks, against which we want to protect the network by disseminating alert messages.

friendly node to launch a *slander attack*. If so, the harm of *slander attacks* is limited. Consider the case that $\tilde{k} = k+1$. Let us compare average message overhead of friendly nodes and that of malicious *slanderers* for different k under *Mobi-Herald* alert propagation protocol in Figure 9. We infer that $k = 3$ is a good choice, since with $k = 3$, each *slanderer* consumes much larger resources than a friendly network node to launch a *slander attack* via illegitimate alert messages. This is because k *slanderers* need to make at least $k + 1$ friendly nodes confirm the alert message in order to successfully launch the *slander attack*. But the number of confirmed nodes grows slowly at the beginning of the alert propagation, because a node needs to collect enough copies of the alert message from different user to confirm the alert message. Hence, under *Mobi-Herald* alert propagation protocol, *slanderers* must take efforts to promote an illegitimate alert message at the beginning. If k is chosen properly, a *slanderer* may consume much more resources than a friendly node to disseminate the illegitimate alert message. From the given scenario, we can see that k does not need to be large to impair *slander attacks* in the system.

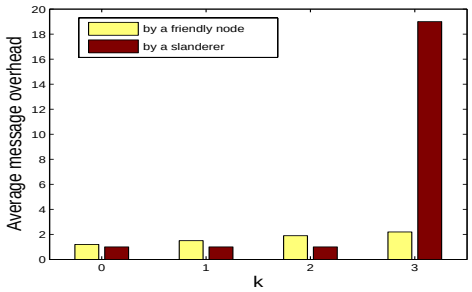


Fig. 9. Comparison of average message overhead, when 600 nodes under *Random Waypoint* mobility model are deployed in a $500meter \times 500meter$ area. Transmission range of each node is $30meter$.

VI. Alert Propagation Management

In previous sections, we introduced *epidemic routing* and *threshold-based verification* schemes in *Mobi-Herald* alert propagation system. In this section, we address another important design issue on how to terminate the alert propagation procedure. If alert propagation of a given message is terminated early, then it is likely that only a portion of the network nodes confirms the alert message. But if the alert propagation procedure is terminated late, then a large amount of bandwidth can be wasted.

As alluded before, *alert propagation management* component determines parameter *TTS*, which controls the termination of alert propagation. We start with deduction of *TTS* value for epidemic routing case, where $k = 0$. We show that for $k = 0$ the *TTS* value has the threshold property that a certain *TTS* ensures almost all network nodes receive the message, but any smaller *TTS* can barely achieve it. Later on, we address the determination of *TTS* for more general case, where $k > 0$.

A. Deduction of TTS for Mobility-assisted Epidemic Routing (without slander attacks ($k = 0$)

To deduce *TTS* with $k = 0$, we assume there are $\mathcal{N}$ nodes in the network and all the nodes remain in an area $\mathcal{A}$ with size $|\mathcal{A}|$ during their mission period. A network node may move arbitrarily within the area $\mathcal{A}$. $P_i(t)$ represents the position of the node i at time t, and $P_i(t) \in \mathcal{A}$. Transmission range of a wireless node is denoted as r. In mobile ad hoc networks, node positions follow continuous processes in continuous time. However, the performance of the *Mobi-Herald* protocol depends on the positions of the mobile heralds when they broadcast the alert message periodically. Hence, our concerns are the snapshot views of the network in different periods with an interval T. If T is large enough to allow a node to move far away from the position in previous snapshot, then in the next snapshot the network nodes are able to mix well with each other. We assume that if the interval T between two snapshot views of the network is large enough (e.g. $v \times T \geq R$), then the position $P_i(t+T)$ is independent of $P_i(t)$ (in Figure 10). This assumption is made for the convenience of the theoretical analysis, however, it is not the requirement of the *Mobi-Herald* protocol. Also for theoretical analysis reasons, we partition incident area $\mathcal{A}$ into hexagons instead of circles. If a node broadcasts a message, all the neighbors within its transmission range r can hear the message. We make an approximation that if a node within the hexagon transmits, all nodes in the hexagon can hear the transmission (Figure 10).

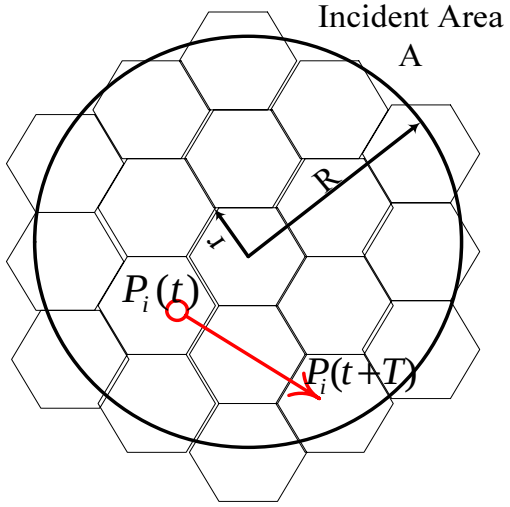


Fig. 10. Illustration of a circle incident area

There are M hexagons covering the incident area $\mathcal{A}$. We estimate $M = \frac{|\mathcal{A}|}{6\times\frac{\sqrt{3}}{4}r^2} \approx \frac{|\mathcal{A}|}{2.6\times r^2}$. Let m be the alert message to be propagated in the network. The expected number of nodes which has received the message m at time t is denoted by $X(t)$, hence $X(t) \geq X(t')$ for $t > t'$ ($X(t)$ is non-decreasing). The *TTS* should be the minimum of δ to make $X(t_0 + \delta T) \approx \mathcal{N}$, where $\mathcal{N}$ is the total number of nodes in the network. Given $X(t_0 + \delta T)$, *Proposition 1* derives the number of alerted nodes $X(t_0 + (\delta + 1)T)$ for the next period. Later on, we utilize *Proposition 1* to derive *TTS* (see *Algorithm 2*).

Proposition 1: The expected number of nodes which have received a given message at time $t_0 + (\delta + 1)T$ satisfies $X(t_0 + (\delta + 1)T) \geq \mathcal{N} \times (1 - e^{-X(t_0+\delta T)\frac{1}{M}})$.
Proof: For $t_0 + \delta T < t < t_0 + (\delta + 1)T$, there are $X(t_0 + \delta T)$ nodes carrying message m. Then the probability that a given hexagon with radius r does not contain any node which has received the message m is $(1 - \frac{1}{M})^{X(t_0+\delta T)}$. Hence, at time $t_0 + (\delta + 1)T$, the expected number of hexagons which contain at least one node carrying the message m is $M(1 - (1 - \frac{1}{M})^{X(t_0+\delta T)})$. Since each hexagon contains $\frac{\mathcal{N}}{M}$ nodes on average, we have:

$$\begin{aligned} X(t_0 + (\delta + 1)T) &= \frac{\mathcal{N}}{M}\{M[1 - (1 - \frac{1}{M})^{X(t_0+\delta T)}]\} \\ &= \mathcal{N} - \mathcal{N} \times (1 - \frac{1}{M})^{X(t_0+\delta T)} \quad (1) \\ &\geq \mathcal{N} \times (1 - e^{-X(t_0+\delta T)\frac{1}{M}}). \square \end{aligned}$$

Note that $X(t)$ is non-decreasing. Based on *Proposition 1*, we device an algorithm to determine *TTS* of the *mobility-assisted* epidemic routing as follows.

Algorithm 2: Estimation of *TTS*

(1) Given network size $\mathcal{N}$ and $M = \frac{|\mathcal{A}|}{2.6 \times r^2}$.

(2) Initialize $\delta = 0$, $X(t_0) = 1$.

(3) While ($X(t_0 + \delta T) < \mathcal{N}$
do { $X(t_0 + (\delta + 1)T) = \mathcal{N} - \mathcal{N}(1 - \frac{1}{M})^{X(t_0+\delta T)}$;
$\delta + +$;
}

(4) Return *TTS* = δ.

Let's consider an example in the circle incident area $\mathcal{A}$ with radius R (in Figure 10), the size of the incident area can be approximated as $|\mathcal{A}| = \pi R^2$. Figure 11 shows the theoretical result of *TTS* depending on density of the network and according to *Algorithm 2*. Our observation is that the proposed *mobility-assisted* epidemic routing protocol is more efficient in a denser network. In Figure 11, *average degree* of a network is defined as the average number of neighbors within the transmission range of a node, so *average degree* indicates node density in a network.

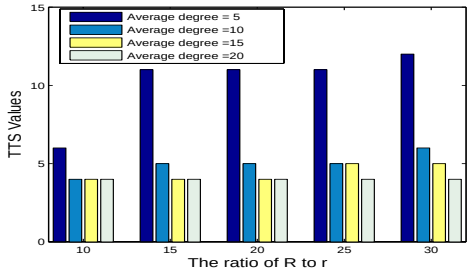


Fig. 11. Analytical results on epidemic routing protocol

Next, we show via simulations that when $k = 0$, the message propagation demonstrates threshold behavior. Let us consider *Random Waypoint* mobility model, and assume square incident area with size $|A| = 500 \times 500m^2$, transmission range $r = 30$ and network size $\mathcal{N} = 600$. According to the analytical result by *Algorithm 2*, we can deduce *TTS=6* for message distribution. In our experiment, among 30 runs of simulations, 29 runs take 6 periods to deliver the message to at least 98% percent of the network nodes (as shown in 12). Only one run takes 5 periods to deliver the message to 98% of all nodes. It shows threshold behavior in the message propagation, so that with $TTS = 6$, almost all nodes receive a copy of the message, but with $TTS < 6$, the chance that the message can be delivered to the whole network is very small. Such threshold behavior implies that an initiator of a message may attach a predetermined value of *TTS* to the message from the beginning of the message propagation procedure, so that the message can be propagated to the whole network within *TTS* periods. We can see that the simulation results and the theoretical analysis agree with each other.

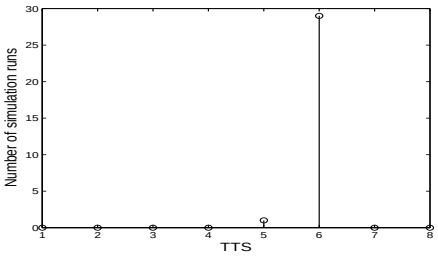


Fig. 12. Probability density function (pdf) of the required *TTS* to achieve 98% coverage for $k = 0$

B. Determination of TTS for Alert Propagation (with individual or colluding slanderers $k > 0$)

Assuming k possible collusive attackers, *Mobi-Herald* alert propagation uses threshold-based verification to defend against collusive *slander attacks*. Only if a node cumulatively hears more than k nodes transmitting the alert message, then the node confirms the alert message. However, we observe that for $k > 0$, *TTS* no longer demonstrates the threshold behavior. For example, Figure 13 shows the distribution of required *TTS* to deliver a message to 98% of network nodes for $k = 2$ ($Q = 3$) case. According to 30 runs of experiments, the required *TTS* for alert propagation varies from 13 to 20 in our experiments. In this case, a predetermined *TTS* cannot guarantee both high coverage of message delivery and low message overhead at the same time. Hence, it is not proper to use a predetermined *TTS* for alert propagation when $k > 0$. Next, we will show how to determine *TTS* based on on-line observation of message transmission.

1) **Proliferation of an Alert Message:** Define $X(t)$ as the expected number of nodes which have received $Q = k + 1$ alert messages and confirm an alert message by time t. We will show that $X(t)$ grows quickly when $X(t)$ is larger than a certain threshold, say N_{TH}^k for k. But before $X(t)$ reaches the threshold, $X(t)$ grows slowly. When $X(t) \geq N_{TH}^k$, we say that the alert message is in the proliferation stage.

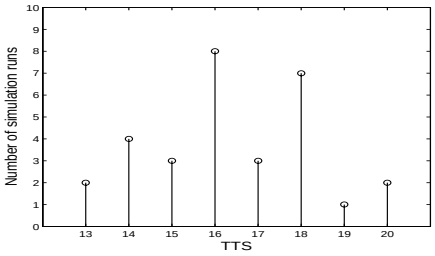


Fig. 13. Probability density function (pdf) of the required *TTS* to achieve 98% coverage for $k = 2$

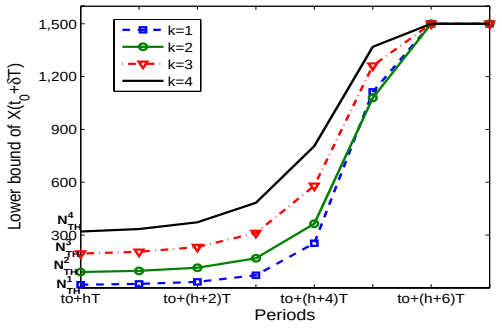


Fig. 14. After $\delta = h$ periods when the expected number of confirmed nodes exceeds a certain threshold N_{TH}^k, the alert message will be propagated to the whole network very soon.

Proposition 2: Let $M = \frac{|\mathcal{A}|}{2.6\times r^2}$ be the number of hexagons covering the incident area $\mathcal{A}$ (see Figure 10). We can infer $X(t_0+(\delta+1)T)$ based on $X(t_0+\delta T)$ as follows:

$$X(t_0+(\delta+1)T) \geq \mathcal{N}\times \sum_{i=k+1}^{X(t_0+\delta T)} \frac{(\frac{X(t_0+\delta T)}{M})^i\ e^{-\frac{X(t_0+\delta T)}{M}}}{i!}$$

Proof: $X(t_0+(\delta+1)T)$ represents the expected number of nodes which have verified the alert message at the $(\delta+1)$-th period. $\frac{(\frac{X(t_0+\delta T)}{M})^i\ e^{-\frac{X(t_0+\delta T)}{M}}}{i!} \approx \binom{X(t_0+\delta T)}{i}(1-\frac{1}{M})^{X(t_0+\delta T)-i}(\frac{1}{M})^i$ represents the probability that a hexagon with radius r contains exactly i nodes which have verified the alert. Therefore, $\frac{\mathcal{N}}{M}\times M\times \sum_{i=k+1}^{X(t_0+\delta T)} \frac{(\frac{X(t_0+\delta T)}{M})^i\ e^{-\frac{X(t_0+\delta T)}{M}}}{i!}$ the number of nodes which have verified the alert by receiving at least $k+1$ copies of an alert message in period $[t_0+\delta T, t_0+(\delta+1)T]$. □

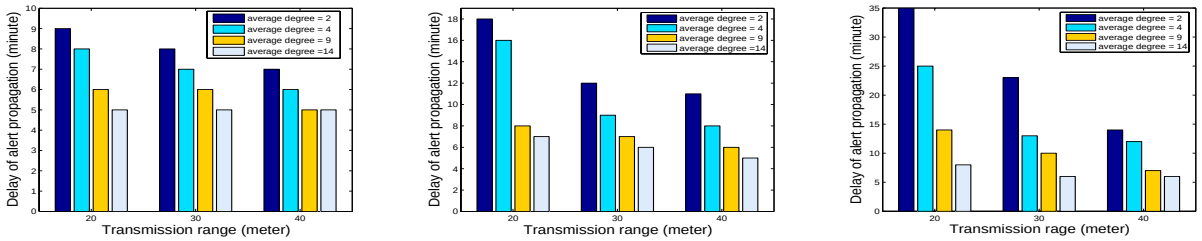
Proposition 2 outlines the lower bound of $X(t_0+\delta T)$ under *Mobi-Herald* alert propagation protocol. This lower bound is obtained in the scenario that a node confirms an alert only when the node hears more than k nodes transmitting the alert message in interval $(t_0+(\delta-1)T, t_0+\delta T]$. In *Mobi-Herald* alert propagation, if a node cumulatively hears more than k nodes transmitting the alert message in interval $[t_0, t_0+\delta T]$, then the node confirms the alert message at time $t_0+\delta T$. Consider a network with $\mathcal{N} = 1500$ nodes, and $M = 100$. According to *Proposition 2*, we calculate the lower bound of $X(t)$. Figure 14 implies that when $X(t_0+\delta T) \geq N_{TH}^k$, $X(t_0+\delta T)$ will reach $\mathcal{N}$ in few periods. This means that as long as the number of confirmed nodes exceeds N_{TH}^k, the alert will be confirmed by almost all the nodes very quickly. In Figure 14, $N_{TH}^1 = 15$, $N_{TH}^2 = 86$, $N_{TH}^3 = 190$, and $N_{TH}^4 = 315$.

Since the proliferation of an alert message implies that the alert message will be propagated to the whole network in a few steps, it can be used to predict the advent of termination of the alert propagation. At the very beginning of *Mobi-Herald* alert propagation (at time t_0), only a few nodes (detectors of malicious behavior) confirm the alert. Hence only a small number of nodes propagate the alert message to their neighborhood. With more and more network nodes having received more than k copies of the alert message, these nodes confirm the alert message and participate in alert propagation. Then, the alert message is proliferated. In the proliferation stage of an alert message, a node is likely to hear $Q = k+1$ transmissions of the alert message in a single period. Here, we take the evidence of $Q = k+1$ transmissions by a node in a single period as an indicator of proliferation of an alert message. Next, we discuss how to terminate the alert propagation, when a node hears Q transmissions in a single period.

2) **Managing TTS for Alert Propagation:** Figure 12 shows that a predetermined *TTS* is not feasible for $k > 0$, since the variation of required *TTS* is large. So the *TTS* value needs to be adjusted based on the on-line detection of the proliferation of an alert message. At the beginning of the alert propagation, we assign a large *TTS* number, say 50, to an alert message m (i.e. set *m.TTS=50*).

While a network node cumulatively receives Q or more copies of the alert message, it confirms the alert message m and begins to propagate m as a herald. At this time, the *epidemic routing* component of the herald node sets its *m.TTS* as the minimum of the received *TTS* values. A herald node reduces its *m.TTS* by one after each transmission period. When any network node observes the proliferation of the alert messages by hearing $Q = k+1$ copies of m in a single period, the node realizes that all network nodes will confirm the alert message m very soon. So the node calculates *TTS* according to *Algorithm 2* by the *alert propagation management* component, and passes the *TTS* value to the *epidemic routing* component. As the *epidemic routing* component receives the *TTS* from the *alert propagation management* component, it updates its *m.TTS* to set *m.TTS*=$min\{$*TTS*,*m.TTS*$\}$.

While hearing transmissions of the alert message by other mobile heralds, a herald node compares the smallest received *TTS* with its own *m.TTS*, and takes the smallest value as its own *m.TTS*. Usually, *Algorithm 2* yields a small *TTS* value comparing to the initially assigned *TTS*. Hence, after a few periods since the first node observes the proliferation of the alert message, the majority of network nodes will reduce their own *m.TTS* values to zero, thus they will terminate the alert propagation procedure. In the case that a very few mobile heralds may not be able to receive the signal (a small *TTS*) to terminate the alert propagation before the rest of the network nodes stop the



(a) $Q = 1$ (b) $Q = 2$ (c) $Q = 3$

Fig. 15. Delay of alert propagation

alert propagation, these herald nodes will keep forwarding the alert message. However, when a friendly node still hears the transmission of alert message after its *m.TTS* reaches zero, it will send a mandatory "STOP" signal to those heralds. Hence, all the herald nodes will be aware of the termination of alert propagation easily.

VII. Evaluation

We have presented *Mobi-Herald* protocol for alert propagation in previous sections, where we derived relevant parameters through theoretical analysis. In this section, we evaluate the performance of the proposed *Mobi-Herald* protocols in terms of the end-to-end delay, the ability to suppress or impair *slanderers*, the coverage (or reliability) of message delivery, and the efficiency of alert propagation through simulations.

A. Simulation Setup

In this section, we investigate the *Mobi-Herald* alert propagation protocol under a commonly used mobility model, *Random Waypoint* mobility model, where a node pauses and moves. A node under *Random Waypoint* mobility model moves from its current position to a new randomly selected location (destination) at a random speed. The pause time of a node is also randomly chosen when it reaches the destination. After the pause time, the node chooses a new destination, speed, and pause time. This procedure is followed by every node until it reaches the end of simulation. We set the maximum pause time as 60 second and the range of moving speed is from $0.5mps$ (meter per second) to $5mps$ in the simulation.

We assume that the ad hoc network spans a square area with edge length $L = 500meter$. We use variant transmission range r and the network size $\mathcal{N}$ to simulate different network diameters and different node densities in the network. We also change threshold value Q to study how Q affects end-to-end delay, coverage of alert message delivery and message overhead in the alert propagation. We randomly select a malicious node and detectors around the malicious node. These detectors generate alert messages regarding the malicious node and serve as mobile heralds to transmit alert messages periodically. The period of message transmission is $T = 1\ minute$.

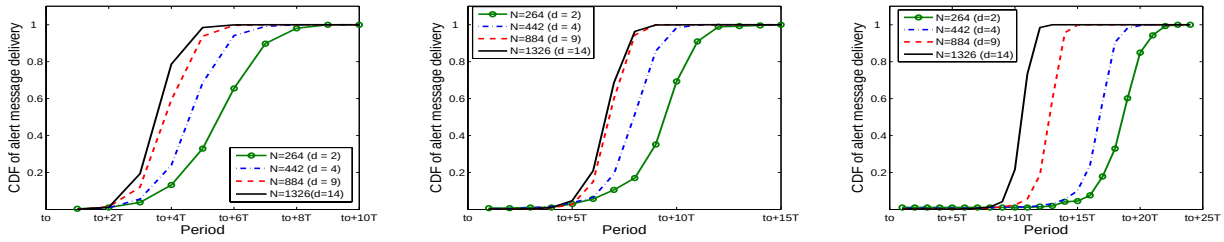
B. End-to-end Delay of Alert Propagation

In the simulation, the delay of the alert propagation is the total time needed to propagate an alert message to the whole network. When $Q = 1$, the alert propagation is reduced to epidemic routing case. The node density of a network is represented by the average degree d. With L, r and network size $\mathcal{N}$, we can estimate $d = \mathcal{N}\frac{L^2}{\pi r^2} - 1$ for circular transmission areas. Figure 15 shows the delay of the alert propagation, which represents how long it will take for all the network nodes to confirm the alert message. Each of the results represents the average of 10 simulation runs. We can observe that the threshold value Q, node density, and transmission range affect the delay of the alert propagation. *First*, the larger Q is, the more copies of a message must be collected before a node actively propagates the alert message. Every node must wait longer time before it confirms an alert message. Hence the delay increases along the threshold value Q. *Second*, we expect a less delay of alert propagation in a denser network, because the denser a network is, the more nodes receive the alert message in each step. *Third*, with the same node density (average degree) and the same Q value, a larger transmission range implies smaller L/r ratio (network diameter), which means that we can use smaller hops to cover the whole network. Hence, it takes a shorter time to propagate an alert throughout the network with a larger transmission range r. With the delays shown in Figure15, majority of network nodes are able to establish defense in time against the detected misbehavior malicious nodes.

C. CDF of Alert Propagation

Let us examine the CDF (Cumulative Distribution Function) of message delivery in *Mobi-Herald* protocol, which demonstrates the probability distribution of confirmed nodes for a given alert message at each period. Figure 16 shows the CDF, when we take the transmission range $r = 30$. It indicates that 100% of network nodes can finally confirm an alert message when *TTS* exceeds a certain value. Also, in a denser network, the CDF of alert message delivery converges to 1 faster. This is because in a denser network, one transmission of an alert message can reach more nodes.

In Figure 16, we observe that the number of confirmed nodes grows slowly at the beginning, but it proliferates when the number of confirmed nodes exceeds a certain threshold and the alert message will be confirmed by the whole network in a few periods. This observation agrees the analytical result we obtained in Section VI-B. Such observation implies that even if Q or more collusive *slanderers* exist in the system, *slanders* must make efforts to promote the illegitimate alert messages at the beginning, in order to launch a *slander attack*. This will damage



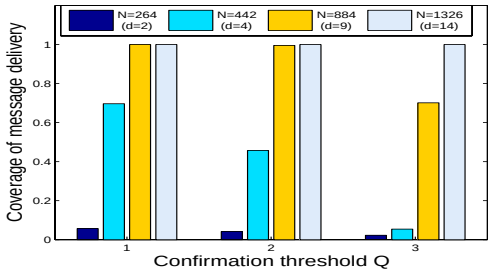
(a) $Q = 1$ (b) $Q = 2$ (c) $Q = 3$

Fig. 16. CDF of alert message delivery under *Mobi-Herald* alert propagation scheme

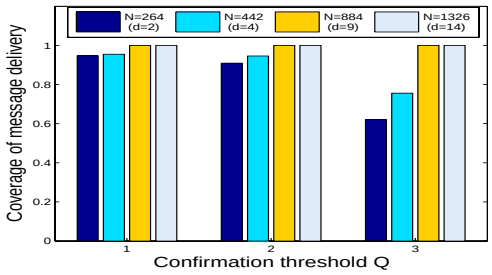
the resource limited *slanderers* themselves. Therefore, we conclude that the *Mobi-Herald* alert propagation protocol is able to fully suppress $Q-1$ collusive *slanders* or impair Q or more collusive *slanders* in an mobile ad hoc network. The larger Q is, the better we can suppress/impair the collusive *slanderers*. However, a larger end-to-end delay and more transmissions will be expected for a larger Q. But as shown in Figure 9, Q does not need to be very large to achieve good performance to suppress/impair collusive *slanderers*.

D. Coverage of Alert Propagation

The coverage of alert propagation exhibits the reliability of the alert propagation. The coverage is measured by percentage of network nodes, which confirm a given alert message by cumulatively receiving at least Q copies of the alert message from different forwarders.



(a) Message delivery coverage by flooding protocol



(b) Message delivery coverage by *Mobi-Herald* protocol

Fig. 17. Comparison of coverage: *flooding* v.s. *Mobi-Herald*

In our *Mobi-Herald* alert propagation protocol, the *Alert Propagation Management* component determines *TTS* value in order to balance the coverage of the alert propagation and message overhead. Here, we investigate the coverage of alert propagation under the proposed scheme. Figure 17 compares the coverage of alert propagation by a *flooding-based* protocol and the *Mobi-Herald* protocol. In the *flooding-based* protocol, upon receiving Q copies of the same alert message assigned by different users, a network node forwards the Q copies of the alert message to its neighbors. Therefore, even if a network node has less than Q neighbors, the node is still able to confirm the alert message in the *flooding-based* protocol. Figure 17(a) and Figure 17(b) illustrate the coverage of *flooding-based* protocol and *Mobi-Herald* alert propagation protocol respectively. d represents the average in the simulation scenarios. Each of the results is based on the average of 10 simulation runs. As Q turns to be large and node density is low, we can see the coverage of alert message delivery under the *flooding-based* protocol can be very low. In contrast, the coverage of alert message delivery is quite encouraging.

E. Communication Efficiency of Alert Propagation

We have shown that *Mobi-Herald* alert propagation protocol achieves high coverage of alert message delivery. Next, we study the message overhead of *Mobi-Herald* protocol. To make a fair comparison of *Mobi-Herald* protocol and the *flooding-based* protocol, we define *normalized message overhead* as the average transmissions needed to cover each network node. The *normalized message overhead* is measured by the ratio of the number of transmissions to the number of confirmed nodes, $i.e.\ Overhead_{msg} = \frac{\#\ of\ transmissions}{\#\ of\ confirmed\ nodes}$.

In the above mentioned *flooding-based* protocol, we can easily conclude that the *normalized message overhead* is Q, since each confirmed node forwards Q copies of the alert message. The *normalized message overhead* of *Mobi-Herald* protocol is obtained through simulations as shown in Figure 18. We observe that only in a sparse network (e.g. average degree of network nodes $d = 2$), the *normalized message overhead* of *Mobi-Herald* protocol is larger than Q. In reasonable dense networks (e.g. $d \geq 4$), *Mobi-Herald* protocol achieves much smaller *normalized message overhead* than that of the *flooding-based* scheme. However, in sparse network the coverage of alert message delivery is very small by the *flooding-based* protocol, and the reliability of alert propagation suffers from frequent network partitions. Since *Mobi-Herald* achieves much better coverage of alert propagation in sparse network, the message overhead of *Mobi-Herald* is satisfactory.

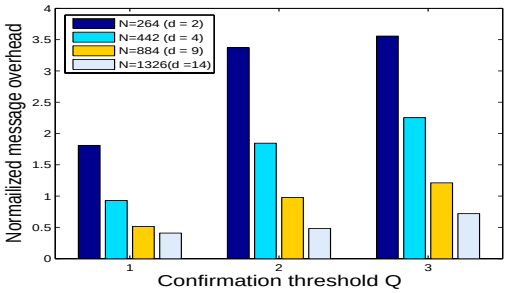


Fig. 18. Normalized message overhead

VIII. Concluding Remarks

The paper presented a novel alert (or message) propagation protocol, which relies on periodically retransmission of the alert messages by mobile network nodes.To prevent the malicious nodes from utilizing alert propagation to issue *DoS* attacks, we adopt a threshold-based verification scheme, where a node confirms an alert only when it has received at least Q copies of the same alert message from different nodes. To use minimum message overhead to achieve network-wide alert message delivery, the transmissions of an alert message is limited by the parameter *TTS*. When $Q = 1$, the *TTS* value demonstrates the threshold property that a certain *TTS* guarantees almost all network nodes confirm the alert, but any smaller *TTS* can barely achieve it. We deduce the value of *TTS* to achieve the threshold behavior by theoretical analysis, and verify it through simulation. When $Q > 1$, there does not exist the threshold behavior. Hence, it is improper to attach a predetermined *TTS* at the beginning of alert propagation. In this case, only when a node detects the evidence of the proliferation of an alert message, it begins attaching a small *TTS* to the alert message. Hence, the alert propagation can be terminated in time to avoid extra bandwidth consumption when the whole network confirms the alert. Our simulation is based on *Random Waypoint* mobility model. The simulation results show that the *Mobi-Herald* alert propagation achieves very high coverage of message delivery with reasonable message overhead and acceptable delay. In the future, we will evaluate *Mobi-Herald* alert propagation protocol with the real world mobility trace.

IX. Acknowledgement

The research in this paper is supported by Motorola grant 1-557641-239016-191100.

References

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in *sixth annual ACM/IEEE International Conference on Mobile Computing and Networking*, 2000, pp. 255–265.

[2] P. Kyasanur and N. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks," *Dependable Computing and Communications Symposium (DCC) at the International Conference on Dependable Systems and Networks (DSN)*, June 2003.

[3] D. Dasgupta, J. Gomez, F. Gonzalez, M. Kaniganti, K. Yallapu, and R. Yarramsettii, "MMDS:Multilevel Monitoring and Detection System," in *Lecture Notes in Computer Science*, ser. Proceedings of the 15th Annual Computer Security Incident Handling Conference, Ottawa, Canada, June 2003.

[4] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, "Flooding for Reliable Multicast in Multi-Hop Ad Hoc Networks," in *Proceedings of the 3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, Seattle, WA, 1999, pp. 64–71.

[5] J. Jetcheva, D. M. Y. Hu, and D. Johnson., "A simple protocol for multicast and broadcast in mobile ad hoc networks," *IETF Internet Draft*, July 2001.

[6] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The Broadcast Storm Problem in A Mobile Ad Hoc Network," in *the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, August 1999, pp. 152–162.

[7] W. Peng and X.-C. Lu, "On the reduction of broadcast redundancy in mobile ad hoc networks," in *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing (MobiHoc)*, 2000, pp. 129–130.

[8] W. Lou and J. Wu, "Double-covered broadcast (DCB): a simple reliable broadcast algorithm in MANETs," in *Proceedings of the 23rd IEEE Inforcom*, March 2004, pp. 2084–2095.

[9] S. Pleisch, M. Balakrishnan, K. Birman, and R. van Renesse, "MISTRAL: efficient flooding in mobile ad-hoc networks." in *Proceedings of the 7th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, May 2006.

[10] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," *Technical Report CS-200006, Department of Computer Science, Duke University*, April 2000.

[11] T. Small and Z. J. Haas, "The shared wireless infostation model - a new ad hoc networking paradigm (or where there is a whale, there is a way)." in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc)*, June 2003.

[12] B. Williams and T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (MobiHoc)*, 2002, pp. 194–205.

[13] Y.-C. Tseng, S.-Y. Ni, and E.-Y. Shih, "Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network," *IEEE Transactions on Computers*, no. 5, pp. 545–557, May 2003.

[14] Q. Zhang and D. P. Agrawal, "Dynamic probabilistic broadcasting in manets," *J. Parallel Distrib. Comput.*, vol. 65, no. 2, pp. 220–233, 2005.

[15] H. Lim and C. Kim, "Multicast tree construction and flooding in wireless ad hoc networks," in *Proceedings of the 3rd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems (MSWIM'00)*. New York, NY, USA: ACM Press, 2000, pp. 61–68.

[16] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad-hoc wireless networks," in *Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2001, pp. 1360–1369.

[17] R. de Moraes, H. Sadjadpour, and J. GarciaLuna, "Throughput-delay analysis of mobile adhoc networks with a multi-copy relaying strategy," in *Proceedings of IEEE SECON*, October 2004.

[18] A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Throughput-delay trade-off in wireless networks," in *Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, March 2004.

[19] G. Sharma, R. R. Mazumdar, and N. B. Shroff, "Delay and capacity trade-offs in mobile ad hoc networks: A global perspective," in *Proceedings of the Twenty-fifth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2006.

[20] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Performance Analysis of Mobility-assisted Routing," in *Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, May 2006.

[21] Z. Zhang, "Routing in Intermittedtly Connected Mobile Ad Hoc Networks And Delay Tolerant Netowrks: Overview And Challenges," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 1, 1st Quarter 2006.

[22] M. Treaster, W. Conner, I. Gupta, and K. Nahrstedt., "ContagAlert: Using Contagion Theory for Adaptive, Distributed Alert Propagation," in *Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications (NCA)*, 2006.

[23] M. Costa, J. Crowcroft, M. Castro, A. Rowstron, L. Zhou, L. Zhang, and P. Barham, "Vigilante: End-to-end Containment of Internet Worms," in *Proceedings of the twentieth ACM symposium on Operating systems principles (SOSP)*, October 2005.