Reliable Privacy-Preserving Communications for Wireless Ad Hoc Networks

Jing Yang Koh[*†], Joseph Chee Ming Teo[†], Derek Leong[†], and Wai-Choong Wong[*]
[*]School for Integrative Sciences and Engineering, National University of Singapore, Singapore
[†]Sense and Sense-abilities Programme, Institute for Infocomm Research, Singapore
Email: jykoh@u.nus.edu, {cmteo, dleong}@i2r.a-star.edu.sg, elewwcl@nus.edu.sg

***Abstract*—We present a phantom-receiver-based routing scheme to enhance the anonymity of each source-destination pair (or contextual privacy) while using an adjustable amount of overhead. We also study how traditional network coding and opportunistic routing can leak contextual privacy. We then incorporated both network coding and opportunistic routing into our scheme for better network performance and show how we mitigate its vulnerability. Contrary to prior works, we allow the destination to anonymously submit an acknowledgment to the source for enhanced reliability. Performance analysis and simulations are used to demonstrate the efficacy of the proposed scheme against commonly considered traffic analysis attacks.**

***Index Terms*—phantom receiver, contextual privacy, global adversary, traffic analysis, network coding, opportunistic routing.**

I. Introduction

Wireless ad hoc networks, such as wireless sensor networks (WSNs), mobile ad hoc networks (MANETs) or vehicular ad hoc networks (VANETs), that rely on wireless communications are exposed to passive traffic analysis attacks which are difficult to detect. Such attacks can leak sensitive *contextual information* [9], [5] (e.g., the location and sender/receiver relationship of communicating parties) about the network traffic patterns and its changes over time to an adversary. In privacy-sensitive applications such as battlefield communications [1], target tracking [2] or surveillance [3] deployments in hostile environments, an adversary may want to derive the source-destination relationship of transmitted messages for malicious reasons. For example, if each soldier in the battlefield carries a wireless node that is used to communicate with its commander, then the adversary can use traffic analysis to trace the location of the latter (destination node).

Although cryptographic mechanisms can be used to protect the message exchanged between two communicating parties, contextual information is easily revealed through traffic analysis. Recent works on privacy-preserving communications [11], [12], [13], [16] have used network coding [6] to improve the network performance and reliability of their routing schemes. In [7], the MORE protocol further combined both network coding and opportunistic routing [8] to sustain a high network throughput despite lossy links. In 2010, the work in [13] provided privacy assurances while building on top of [7]. However, we show in the following example how network coding with opportunistic routing can leak contextual information.

The work of J. Y. Koh was supported by the Agency for Science, Technology and Research (A*STAR) Graduate Scholarship. The work of J. C. M. Teo was supported in part by A*STAR, Singapore, under SERC Grant 1224104047. The work of D. Leong was supported in part by A*STAR, Singapore, under SERC Grant 1224104049.

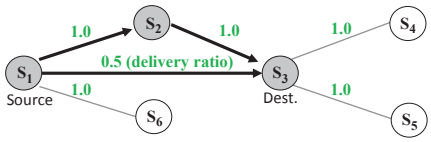


Fig. 1. Example of how opportunistic routing leaks contextual privacy. The lines connecting two nodes represent communication links and the numbers beside each link represent the link delivery ratio.

Motivating Example. In opportunistic routing, the next hop receiver is dynamically chosen so each packet may travel through different paths to reach its destination. However, from the point of view of an adversary, the use of opportunistic routing forwarder nodes can decrease the set of possible destination candidates which lowers the contextual privacy of the destination. This is because the forwarder nodes must have a common intersection region at the destination. We illustrate how network coding when used with opportunistic routing (e.g., [7], [13]) can leak privacy in the network shown in Fig. 1. We chose an arbitrary network topology which can be generalized to other topologies where both network coding and opportunistic routing are used. Assume that source node S_1 wants to transmit 10 packets to a single destination node S_3 via the shortest path. Using network coding and opportunistic routing as described in [7], S_1 broadcasts 10 coded packets and S_2 broadcasts 5 coded packets (on average) to S_3. Node S_3 can decode the original 10 packets from any 10 received independently coded packets due to the property of network coding. However, an observer who is aware of the scheme being used can correlate the traffic pattern to deduce that S_3 is the destination due to S_2's transmissions. Without opportunistic routing, S_1 will need to transmit 20 coded packets (on average) to S_3 in order for it to decode the packets. Now, the observer only has $\frac{1}{3}$ (random guess) probability of guessing the correct destination since all 3 one-hop nodes S_2, S_3, and S_6 are possible destination candidates. But if we allow S_3 to probabilistically forward the packets (e.g., to S_4 and S_5) then all S_2, S_3, S_4, S_5, and S_6 are now the potential destination. The observer now has a $\frac{1}{5}$ chance of correctly guessing the destination. S_3 can still receive the packets with low latency as the shortest path is used. Thus, if the source node probabilistically routes messages to

such randomly selected *phantom receivers* (e.g., S_4, S_5 in our example) with the destination hidden en route, then contextual privacy is enhanced as the destination is now hidden among a larger set of possible candidates.

Our Contribution. In this paper, we propose a phantom receiver based routing scheme to provide communication *unlinkability* [13], [16] for enhanced contextual privacy. Our scheme leverages on the network coding and opportunistic routing techniques for better network performance. It can mitigate advanced traffic analysis techniques while avoiding costly communication overheads due to flooding or periodic broadcasts. Our contributions are summarized as follows:

1) We propose an algorithm to enhance communication unlinkability through the use of phantom receivers.
2) Our solution is able to mitigate a strong global adversary who is able to monitor the network traffic, compromise nodes, and selectively drop packets.
3) Our solution provides communication reliability using anonymous acknowledgement packets.

The rest of this paper is organized as follows: Section II presents the related work and Section III describes the system models. The proposed scheme is presented in Section IV, security analysis in Section V and simulation results in Section VI. Finally, Section VII concludes the paper.

II. Related Work

The location privacy issue in wireless networks has been widely studied in the area of wireless sensor networks (WSNs). We classified existing privacy-preserving schemes into non-network coding (NC) based [4], [5], [9], [10] and NC-based [11], [12], [16], [13]. In [4], the importance of location privacy in WSN was highlighted and a directed walk based phantom routing scheme was proposed to protect the source location privacy. The source first sends the message via a directed walk to a phantom source which then floods the message to the destination. Subsequently, [9] proposed a more efficient scheme which randomly injects dummy packets into the routing path to create multiple routes. Next, [5] used both fake sources and receivers to periodically generate dummy traffic to provide anonymity for both the source and destination. In [11], the authors employed homomorphic encryption with NC to enhance privacy. They highlighted that NC provides an intrinsic mixing feature similar to a Mix-Net which mitigates traffic analysis techniques such as packet size, time and content correlation. In a Mix-Net, a set of "mix" nodes will reorder and mix transmitted messages as they traverse through. However, a Mix-Net requires the existence of multiple concurrent flows to be effective. Thus, [12] proposed a decentralized scheduling algorithm and used multiple dummy traffic flows to exploit the intrinsic mixing feature of network coding for better anonymity. Similarly, [16] introduced the Onion Routing concept into network coding to provide unlinkability. Finally, [13] proposed an anonymous routing scheme which utilizes both NC and opportunistic routing (OR) to improve network performances in lossy links. Such routing techniques are useful in many practical wireless networks since the wireless channels are usually lossy. The authors then proved that the scheme is resilient against statistical traffic analysis attacks. However, as discussed in the example in our introduction, such schemes are still vulnerable to traffic analysis attacks.

III. System Model

Our goal is to ensure that the destination is hidden among a set of possible candidates (also known as an anonymity set [10]) denoted by $\boldsymbol{\mathcal{D}}_{\text{candidate}}$. We first present the system and adversarial models before discussing our solution.

A. Network Model

Assume an ad hoc network and uni-cast routing (only one source and one destination per communication flow). Let the wireless network be modeled as a connected graph $\boldsymbol{\mathcal{G}} = (\boldsymbol{\mathcal{V}}, \boldsymbol{\mathcal{E}})$, where $\boldsymbol{\mathcal{V}}$ is the set of N nodes and $\boldsymbol{\mathcal{E}}$ represents the set of undirected $\{S_i, S_j\}$ communication links between nodes where $S_i, S_j \in \boldsymbol{\mathcal{V}}$. Suppose a source node S_{src} wants to transmit a message to the destination node S_{dest}. Let $\boldsymbol{\mathcal{F}} = (S_{\text{src}}, S_1, \cdots, S_k)$ denote the routing path taken from the source to destination where $S_i,\ i = 1, \cdots, k$ are the identities of the nodes that transmitted in the communication flow. $\boldsymbol{\mathcal{F}}$ can be viewed as a sequence of transmissions in the communication flow consisting of k forwarder nodes.

Definition 1 (Potential destination candidates, $\boldsymbol{\mathcal{D}}_{\text{candidate}}$)**.** *All nodes S_j that have received the transmitted message in the communication flow $\boldsymbol{\mathcal{F}}$ are potential destination nodes. i.e.,* $\boldsymbol{\mathcal{D}}_{\text{candidate}} = \bigcup_{S_k \in \boldsymbol{\mathcal{F}}} \left\{ S_j \,:\, \{S_j, S_k\} \in \boldsymbol{\mathcal{E}} \right\} \backslash \{S_{\text{src}}\}$.

B. Adversarial Model

The adversary's goal is to minimize the set of destination candidates $\boldsymbol{\mathcal{D}}_{\text{candidate}}$ so as to locate the destination node and compromise contextual privacy. We consider a *global, internal* and *active* adversary who is able to observe all wireless traffic in the network, compromise nodes and actively modify traffic. Such powerful global observer models have been used in [5], [11], [12], [13], [16]. Given a specific communication flow, we assume that the global adversary (GA) observes the complete set of transmission activities in the flow denoted by $\boldsymbol{\mathcal{F}}_{\text{GA}}^{\text{obs}}$ such that $\boldsymbol{\mathcal{F}}_{\text{GA}}^{\text{obs}} = \boldsymbol{\mathcal{F}}$. Suppose the adversary has knowledge of $\boldsymbol{\mathcal{G}}$, he can perform both passive and active traffic analysis attacks (discussed in Section V) to derive and minimize $\boldsymbol{\mathcal{D}}_{\text{candidate}}$. Note that if our scheme is able to mitigate the global adversary (GA) then it can also mitigate a "weaker" local adversary (LA) which only observes a subset of transmission activities in the flow $\boldsymbol{\mathcal{F}}_{\text{LA}}^{\text{obs}}$ such that $\boldsymbol{\mathcal{F}}_{\text{LA}}^{\text{obs}} \subseteq \boldsymbol{\mathcal{F}}_{\text{GA}}^{\text{obs}}$. This is because there may exist a scenario where the local adversary is unable to include the destination node in the suspected $\boldsymbol{\mathcal{D}}_{\text{candidate}}$ as the former was not observed to have received the transmitted message.

IV. Privacy-Preserving Communications with Encoded Opportunistic Routing

We present our proposed scheme that enhances communication *unlinkability* [13], [16] of the communicating parties. The general idea of our scheme is to make use of *phantom receivers* S_p(s) to introduce some randomness in the routing path and

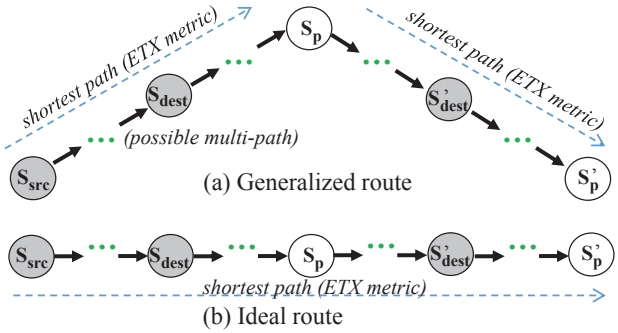


Fig. 2. Visualization of the proposed route selection. S_{src} denotes source, $S_{\text{dest}}, S'_{\text{dest}}$ denote destination, and $S_{\text{p}}, S'_{\text{p}}$ denote phantom receiver. The destination node can either be in S_{dest} or S'_{dest} but not both.

hence, increase the set of possible destination candidates $\mathcal{D}_{\text{candidate}}$. Our scheme is built upon the network coding-based opportunistic routing protocol, MORE [7]. As discussed earlier, a major limitation of the shortest path routing is that the destination always lies at the end of the taken route. Hence, $\mathcal{D}_{\text{candidate}}$ is very limited. To overcome this, we allow the destination to randomly forward the message to random phantom receivers as shown in Fig. 2 where the former can either be S_{dest} or S'_{dest}. From an observer's point of view, the destination can be any of the nodes that received the message.

The proposed scheme consists of three phases: (i) the route construction, (ii) the data transmission, and (iii) the anonymous acknowledgment (ACK) phases. In the route construction phase, the source node constructs a privacy-preserving phantom receiver route and identifies the potential forwarder nodes (including phantom receivers) for the route. Next, the source uses an initial Route Setup (RS) packet to inform all the forwarder nodes of their next hop receivers. The RS packets are designed in such a way that each forwarder is only aware of its previous and next hop nodes but not the entire routing path. In the data transmission phase, the source computes network coding and uses a modified MORE protocol [7] to transmit the coded packets along the computed route. Specifically, we removed the forwarder's list embedded in each data packet and removed the use of the explicit acknowledgment (ACK) packets to enhance its privacy. They are replaced by the Route Setup (RS) and anonymous ACK packets respectively and will be discussed in the following subsections. Finally, in the anonymous ACK phase, the last node in the route (not necessarily the destination) will transmit a special ACK packet along the reverse direction of the previously traversed route. This special ACK packet prevents leakage of the destination's identity and at the same time allows the destination to anonymously acknowledge to the source.

We assume that each node has three types of cryptographic keys: a pairwise encryption and authentication key shared with every other node in the network and a cluster key shared with all its one-hop neighbors. Each transmitted message to a destination is encrypted using the shared pairwise key to provide content privacy and includes a short message authentication code (MAC) to provide both end-to-end authenticity and integrity checks. In addition, we use hop-by-hop encryption using the cluster keys to mitigate simple content correlation attacks and we divide all coded packets into equal sizes to prevent packet size correlation attacks.

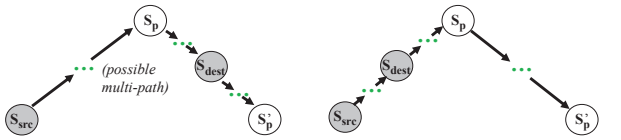
input : source node S_{src}, destination S_{dest}, random steps $\mathcal{M}_{\text{steps}}$, max hops $\mathcal{M}_{\text{hops}}$, network graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$;
output : communication flow $\mathcal{F}$;
initialize : phantom receivers, $S_{p1} \leftarrow S_{\text{dest}}$, $S_{p2} \leftarrow S_{\text{dest}}$, $h_{\text{hops}} \leftarrow \text{rand\_int}(0, \mathcal{M}_{\text{hops}})$;
// Compute random walk from S_{dest} for $\mathcal{M}_{\text{steps}}$ random steps
// to select the first phantom receiver, S_{p1}.
for $i = 0; i < \mathcal{M}_{\text{steps}}; i++$ **do**
    $S_{p1} \leftarrow$ random one-hop neighbor of S_{p1};
end
if $\text{euclidean\_dist}(S_{\text{src}}, S_{p1}) < \text{euclidean\_dist}(S_{\text{src}}, S_{\text{dest}})$ **then**
    // Route to phantom first.
    $\mathcal{F} \leftarrow \text{etx\_path}(S_{\text{src}}, S_{p1})$;
    // Route from phantom to destination.
    $\mathcal{F} \leftarrow \mathcal{F} \cup \text{etx\_path}(S_{p1}, S_{\text{dest}})$;
    // Route from destination to phantom.
    Find S_{p2} such that $S_{\text{dest}} \in \text{etx\_path}(S_{p1}, S_{p2})$
    $\mathcal{F} \leftarrow \mathcal{F} \cup \text{etx\_path}(S_{\text{dest}}, S_{p2})$;
else
    // Route to destination first.
    $\mathcal{F} \leftarrow \text{etx\_path}(S_{\text{src}}, S_{\text{dest}})$;
    // Route from destination to phantom.
    Find S_{p2} such that $S_{\text{dest}} \in \text{etx\_path}(S_{\text{src}}, S_{p2})$
    $\mathcal{F} \leftarrow \mathcal{F} \cup \text{etx\_path}(S_{\text{dest}}, S_{p2})$;
    // Route from phantom to phantom.
    $\mathcal{F} \leftarrow \mathcal{F} \cup \text{etx\_path}(S_{p2}, S_{p1})$;
end

Algorithm 1: Phantom Receiver Route Selection.

A. Route Construction Phase

The source node S_{src} uses Algorithm 1 to compute a privacy-preserving route to its destination. The functions $\text{etx\_path}(S_i, S_k)$ outputs the list of forwarder nodes along the shortest path (using the ETX metric [8]) from node S_i to S_k (excluding S_k), $\text{rand\_int}(0, n)$ outputs a random integer from 0 to n (inclusive), $\text{euclidean\_distance}(S_i, S_k)$ outputs the euclidean distance (in hop count) from S_i to S_k, and // denotes comment. Ideally, the computed route should be the shortest path (in terms of ETX metric [8]) from the source to the last forwarder node as shown in Fig. 2b. However, our scheme also accommodates the scenario given in Fig. 2a where the destination is a leaf node near the edge of the network.

In Algorithm 1, the source first virtually computes a random walk with $\mathcal{M}_{\text{steps}}$ number of "steps" (or hops) from the destination to a phantom receiver S_{p}. Next, depending on whether the phantom receiver S_{p} is closer to the source or the destination, the packets are routed separately as shown in Fig. 3. In Fig. 3(a), the packets are routed to the phantom receiver S_{p} first as the latter is closer to the source than the destination. The phantom receiver S_{p} then forwards the packets to the destination S_{dest} which may then probabilistically forward the packets to another phantom receiver S'_{p} along the ETX shortest path for a maximum of $\mathcal{M}_{\text{hops}}$ number of hops. Otherwise, packets are routed to the destination first as shown in Fig. 3(b). Hence, the destination may lie within both



(a) Route to phantom S_p first (b) Route to destination S_{dest} first

Fig. 3. Two possible routing scenarios.

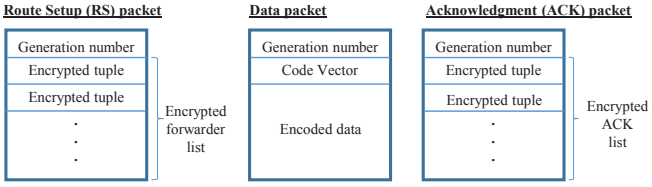


Fig. 4. Route setup, data and acknowledgment packet structures.

the left and right portions of the taken route (see Fig. 3), and it can be any of the intermediate forwarder nodes since the destination can probabilistically continue forwarding the packets. Each source node should be assigned independent $\mathcal{M}_{\text{steps}}$ and $\mathcal{M}_{\text{hops}}$ parameters so that the compromise of one node does not leak the parametric information of the other nodes. Both parameters can be estimated using simulations according to the specific network topology and the desired network performance-anonymity trade-off.

Initial Route Setup (RS) Packet: After computing the route to the destination, the source S_{src} sends an initial uncoded RS packet to each forwarder node to anonymously inform each forwarder node of its next hop receivers. The RS packet contains (i) the generation number range, and (ii) the forwarder list in the form of many encrypted Enc("$S_{\text{src}} \rightarrow S_k : x$", $K_{\text{src,j}}$), $\cdots$ tuples where Enc("m", $K_{\text{src,j}}$) denotes an encryption of content m with the encryption key $K_{\text{src,j}}$ shared between the source and each forwarder node j and x is the number of packets that the preceding node wants to transmit to the next hop receiver S_k (used by our underlying MORE protocol, see Section 5.1 of [7]). Each selected forwarder f is able to decrypt a tuple e.g., Enc("$S_j \rightarrow S_k : x$", $K_{\text{src,f}}$) and receive its routing instructions while other unselected nodes are unable to gain any information from the packet. The destination S_{dest} will receive a different tuple, Enc("dest : $S_j \rightarrow S_k : x$", $K_{\text{src,dest}}$) to indicate that it is the destination. Similarly, the last forwarder node l will receive the tuple, Enc("ACK to S_{src}", $K_{\text{src,l}}$) to indicate that it should send an ACK packet. Finally, each forwarder node saves the received routing instructions for a specified period of time and forwards the RS packet to its designated next hop receiver(s). This approach was chosen over the Onion Routing as used in [16] because the latter is unable to accommodate opportunistic routing (OR) since the layered encryptions must be sequentially removed and cannot tolerate the possible multi-path routes taken in OR. Our approach is superior to a similar trapdoor-based encryption scheme used in [13] where the source computes the exact number of transmissions for each forwarder to broadcast. The latter limits the effectiveness of OR as the link rates may change dynamically.

B. Data Transmission Phase

Next, the source encrypts the data with the key shared with the destination and transmits the actual coded data packets to the destination. The data to be sent is encrypted before the packet encoding and splitting. Each data packet consists of a packet header containing (i) the generation number, and (ii) code vector as shown in Fig. 4. Each forwarder node that receives a coded packet from the generation number it is supposed to forward will check the packet for innovativeness (see [7]). Innovative packets contain useful information to allow the receiver to decode the original message. Such packets are then forwarded by the forwarder node to its designated receivers using the modified MORE protocol. Otherwise, a non-innovative packet is dropped.

C. Anonymous Acknowledgment (ACK) Phase

The last forwarder node in the flow will transmit an ACK packet once it received all the transmitted packets. The ACK packet will travel in the reverse direction of the previously traversed route. Each forwarder node in the route sequentially appends a dummy tuple to the received ACK packet. A second ACK packet is created when the initial packet is full but each node only appends the tuple once. The destination however, will append the tuple Enc("ACK g", $K_{\text{src,dest}}$) where g is the generation number if it has successfully decoded the message. The source can check the existence of the destination's tuple as it is encrypted using a shared symmetric key. Otherwise, the source may re-transmit more coded packets until the destination is able to decode. Usually, the sending of ACK packets can quickly reveal the destination. However, anonymity is provided here as each forwarder node (including the destination) will append an encrypted tuple to the ACK packet.

V. Security Analysis

We discuss how the our scheme is able to mitigate both passive and active traffic analysis attacks. The following attacks were also used in the literature [9], [11], [15], [16]:

A. Passive Traffic Analysis Attack Mitigation

Time correlation attack [9], [11], [15]: an adversary correlates the packet transmission times to trace the packet from its source to its destination. An example of how such an attack can be implemented is for the adversary to record all the nodes that received the transmitted packet in the route. If shortest path is used, then the destination node should be among the nodes that only received the transmission from the last transmitting node and not those which received the transmissions by the previous forwarder nodes. However, this assumption is not true in our scheme. The destination is hidden inside a large $\mathcal{D}_{\text{candidate}}$ which consists of all forwarder nodes that have received the packet. This is because the destination can probabilistically forward the packet to other phantom receivers. Hence, the discovery of the entire routing path itself does not leak further information on the destination as the latter may not be at the end of the route.

Rate monitoring attack [15]: an adversary observes the wireless traffic and guesses that the destination node lies within the region of higher packet transmission rates. Such attacks do not affect our scheme if the communication flows are independent (source communicates with different destinations each time). However, if the flows are dependent (e.g., source is alway sending to a fixed destination), then specific traffic patterns may be observed over a long period of time. Hence, fixed phantom receivers should be selected by the source if it intends to communicate with a destination node for extended periods of time. This helps to mislead the adversary by diverting the region of high transmission counts away from the destination. Although the adversary may guess that the source is communicating with the same receiver, he is unable to pinpoint the exact destination node. We use simulations to evaluate the effectiveness of such attacks in Section VI-A.

B. Active Traffic Analysis Attack Mitigation

External adversarial attack: the adversary selectively drops or delays packets to create specific traffic patterns to facilitate packet tracing. This allows the adversary to identify the routing path taken. However, no vital information about the destination is leaked in our scheme as the destination is still hidden in $\mathcal{D}_{\text{candidate}}$. The adversary is unable to replay a specific packet in another part of the network or selectively prevent suspected destination nodes from submitting their ACK tuples as all packets are authenticated via hop-by-hop encryptions. In order for the destination to acknowledge the received message, all intermediate nodes (including the destination itself) must have received all the packets transmitted by the source. Otherwise, the last forwarder node will not initiate the ACK packet. Therefore, since all the forwarder nodes in the route have received the transmitted message, each of them can potentially be the destination node.

Internal adversarial attack [11], [16]: the adversary compromises some intermediate nodes and analyses the traffic passing through them. Despite being able to read the packet header information, the adversary is unable to identify the destination node as each forwarder node only knows its previous hop sources and next hop receivers and does not have knowledge of the destination. Also, the adversary is unable to retrieve the transmitted contents to the destination as they are encrypted using a pairwise key shared with the destination.

VI. Simulation

We simulate a 50-node wireless ad hoc network in a 100m×100m area where the nodes are randomly placed with a minimum distance of 5m apart. We simulate both a sparsely and densely connected networks. The communication range of each node is 17m for a (i) sparse network where each node has few one-hop neighbors (mean 3.54, standard deviation of 0.31), and 29m for a (ii) dense network where the nodes have more one-hop neighbors (mean 9.42, standard deviation of 0.72). A single source and destination pair is randomly chosen and we evaluated the anonymity of the following routing schemes under the time correlation and rate monitoring attacks:

1) baseline shortest path by hop counts,
2) random walk (LPR scheme from [9] with $p_f = 50\%$),
3) A-WEOR [13] which uses network coding with opportunistic routing,
4) our proposed scheme with parameters $\mathcal{M}_{\text{steps}} = 10$ and $\mathcal{M}_{\text{hops}} = 2$.

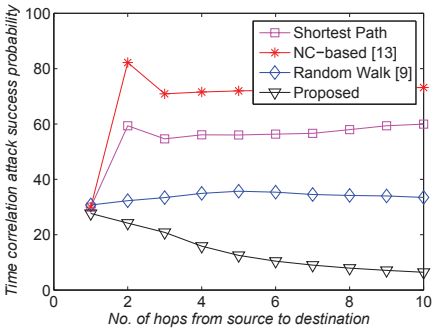


Fig. 5. Probability of time correlation success (sparse network).

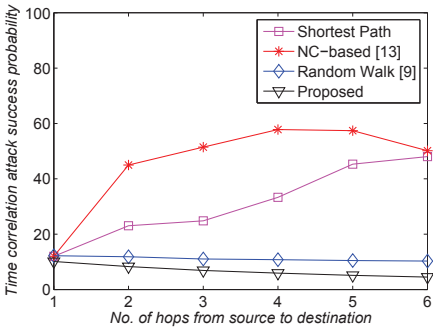


Fig. 6. Probability of time correlation success (dense network).

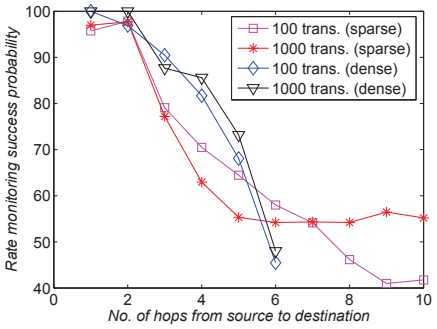


Fig. 7. Probability of rate monitoring success in proposed scheme.

A. Simulation Results

We use the success probability of the described traffic analysis attack to measure the level of anonymity provided by the scheme. Figs. 5 and 6 show the success probability of the time correlation attack (given by $\frac{1}{|\mathcal{D}_{\text{candidate}}|}$) for communication flows in the sparse and dense network environment respectively against the latency (or least number of hops to destination). We used a modified time correlation attack as explained in our introduction to derive the set of destinations candidates $\mathcal{D}_{\text{candidate}}$ when opportunistic routing and network coding are used. As shown in Fig. 5, our scheme provides the highest level of anonymity (lower attack success rate) under

the time correlation attack compared to the other schemes in a sparsely connected network. As $\mathcal{D}_{\text{candidate}}$ is proportional to the length of the taken route for our scheme, the level of the anonymity in our scheme improves as the destination is located further away. At one hop distance, all schemes provide similar levels of anonymity as all the one-hop neighbors can be the destination candidates. The little spike at two hop is due to the abrupt decrease in $\mathcal{D}_{\text{candidate}}$ which only consist of the "new" nodes that received the transmission from the last forwarder node. The amount of anonymity provided tends to be consistent as the number of hops increase further.

In Fig. 6, our scheme provides the highest level of anonymity against the time correlation attack in the densely connected network. However, we observe that the level of anonymity provided by the other schemes in the denser network has improved. This is because a denser network naturally provides a larger $\mathcal{D}_{\text{candidate}}$ as each node has a higher number of one-hop neighbors. Hence, despite the fact that the destination always lies at the end of the routing path in the other schemes, there are still many potential destination candidates due to the increased number of one-hop neighbors. Generally, the anonymity provided by the other schemes is at its highest when the destination is one-hop away from the source as explained earlier.

Information about the destination may be leaked using rate monitoring attacks if the communication flows are dependent. We simulate the scenario where the source continuously sends multiple independent messages (both 100 and 1000) to the same destination. The rate monitoring attack success for our scheme is given in Fig. 7. We do not show the results for the other three schemes as the rate monitoring attack success probability is near 100% due to the predictable nature of their routes. In the random walk and opportunistic routing based schemes, the various traversed paths will eventually converge near the destination. This greatly improves the success probability of the rate monitoring attack. In our scheme, the attack success rate is higher when the source is 1-3 hops away from the destination and decreases significantly as the destination lies further away. This is because the phantom receivers are more dispersed at larger distances, resulting in a more evenly distributed traffic pattern which impedes rate monitoring attempts. Because the number of nodes in the network is fixed, the maximum number of hops to the destination in the dense network is lesser than that of the less dense network.

Different from prior works which may rely extensively on periodic dummy traffic generation for privacy protection, our scheme is able to provide better anonymity with better energy-efficiency because it only generates additional traffic probabilistically according to the selected parameters.

VII. Conclusion and Future Work

In this paper, we present a privacy-preserving routing scheme to enhance contextual privacy. The main features include the use of phantom receivers to overcome the traffic analysis vulnerability of network coding and opportunistic routing, and the use of anonymous acknowledgments for reliability. Simulation results and analyses show the efficacy of the proposed scheme when compared to other schemes. Future work would be to implement the proposed scheme in a testbed to demonstrate its practicality and optimize the routing algorithm to accommodate latency-constrained, energy-constrained and mobile applications. It would also be interesting to study the anonymity-cost trade-off in greater detail.

References

[1] K. El Defrawy and G. Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs," in IEEE J. Sel. Areas Commun., vol. 29, no. 10, pp. 1926-1934, Dec. 2011.

[2] R. Hartwell, "Wireless Sensor Network Energy Use While Tracking Secure Area Intrusions," in *IEEE MILCOM*, pp. 1696-1701, Nov. 2013.

[3] E. Onur, C. Ersoy, H. Delic, L. Akarun, "Surveillance Wireless Sensor Networks: Deployment Quality Analysis," in *IEEE Network*, vol.21, no.6, pp. 48-53, Nov. 2007.

[4] C. Ozturk, Y. Zhang, W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *ACM workshop on Security of Ad hoc and Sensor Networks (SASN)*, pp. 88-93, 2004.

[5] K. Mehta, D. Liu, M. Wright, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper," in *IEEE Trans. on Mobile Comput.*, vol. 11, no. 2, pp. 320-336, Feb. 2012.

[6] R. Ahlswede, C. Ning, S.-Y.R. Li, R.W. Yeung, "Network information flow," in *IEEE Trans. on Inf. Theory*, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.

[7] S. Chachulski, M. Jennings, S. Katti, D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *ACM SIGCOMM*, pp. 169-180, Aug. 2007.

[8] S. Biswas and R. Morris, "ExOR: opportunistic multi-hop routing for wireless networks," in *ACM SIGCOMM*, pp. 133-144, Oct. 2005.

[9] Y. Jian, S. Chen, Z. Zhang, L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," in *IEEE Trans. on Wireless Commun.*, vol. 7, no. 10, pp. 3769-3779, Oct. 2008.

[10] X. Hong, P. Wang, J. Kong, Q. Zheng, J. Liu, "Effective probabilistic approach protecting sensor traffic," in *IEEE MILCOM*, pp. 169-175, Oct. 2005.

[11] Y. Fan, Y. Jiang, H. Zhu, J. Chen, X. Shen,"Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks," in *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 834-843, Mar. 2011.

[12] Z. Wan, K. Xing, Y. Liu, "Priv-Code: Preserving privacy against traffic analysis through network coding for multihop wireless networks," in *IEEE INFOCOM*, pp. 73-81, Mar. 2012.

[13] N. Shah and D. Huang, "A-WEOR: Communication Privacy Protection for Wireless Mesh Networks Using Encoded Opportunistic Routing," in *IEEE INFOCOM*, pp. 1-6, Mar. 2010.

[14] S. Douglas, D. Aguayo, J. Bicket, R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *ACM MobiCom*, pp. 134-146, 2003.

[15] J. Deng, R. Han, S. Mishra, "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks," in *Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm)*, pp.113-126, Sep. 2005.

[16] P. Zhang, C. Lin, Y. Jiang, P.P.C. Lee, J.C.S. Lui, "ANOC: Anonymous Network-Coding-Based Communication with Efficient Cooperation," in *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1738-1745, Oct. 2012.