DOI: 10.1109/LCOMM.2019.2927913

Privacy-Preserving Forwarding using Homomorphic Encryption for Information-Centric Wireless Ad Hoc Networks

Carlos Borrego, Marica Amadeo, Antonella Molinaro, Rutvij H. Jhaveri

Abstract—**In order to improve the forwarding performance of the Information-Centric Networking (ICN) paradigm in wireless ad hoc environments, different nodes' properties, such as geographical position and topological centrality, have been proposed as metrics to identify the suitability of a node as a forwarder. However, while these metrics may be efficient in terms of node selection, they can breach the privacy of the node itself. The more efficient these metrics are, the more private information they may reveal. In this letter, we propose a privacy-preserving ICN forwarding scheme based on homomorphic encryption for wireless ad hoc networks.**

Index Terms—**Privacy, Information-Centric Networking, Named Data Networking, Forwarding, Homomorphic Encryption**

I. Introduction

Direct wireless ad hoc connections among mobile user devices, such as smartphones, are expected to play a crucial role in future telecommunication networks and the Internet, by enabling a variety of groundbreaking applications in the areas of the Internet of Things (IoT) and edge computing. In such a challenging scenario, networking, security and privacy aspects are deemed crucial.

In the last few years, the research community has focused on the revolutionary Information-Centric Networking (ICN) [1] paradigm, and in particular on its Named Data Networking (NDN) instantiation [2], as an effective solution to support content retrieval and dissemination in ad hoc environments [3]. Unlike the IP communication that is based on the "topology-dependent" IP addresses of end nodes, NDN communication is based on "names" given to the content hosted by the nodes [2]. As a result, the NDN layer uses names for content search and retrieval that are independent of the hosting node's physical location. In-network caching is natively supported by NDN, which is especially useful in situations of intermittent wireless connectivity. A lightweight connectionless forwarding mechanism is supported based on two packet types, the *Interest* and the *Data*, respectively exchanged between data consumers and providers. Consumers broadcast Interest packets carrying the name of the requested content Each receiving node first checks for a locally stored content copy to send back and, in case of failure, it continues the packet forwarding.

Some smart forwarding protocols for NDN wireless ad hoc networks have been proposed in the literature [3], which select the best next-hop forwarder(s) based on given node-related metrics (e.g., position, topological or social centrality) piggybacked into Interest/Data packets [4], [5]. In those protocols, however, metrics are exchanged as a clear text, thus potentially compromising the privacy of the network users. By collecting the NDN packets piggybacking the forwarding metrics, a malicious entity may infer personal information of the user, like where she lives or where she works.

Existing solutions for privacy-preserving ICN forwarding have been devised for wired environments [6] and they cannot be straightforwardly applied in ad hoc networks. For instance, the works in [7] and [8] rely on specific entities responsible for client privacy, which are generally not available in the dynamic, mobile and usually stand-alone ad hoc scenarios.

To fill this gap, we propose an NDN Privacy-Preserving Forwarding (NDN-P^2F) scheme that provides the following original contributions: *(i)* it focuses on privacy-preserving forwarding in the challenging NDN wireless ad hoc environment and it defines a *distributed* scheme that mobile nodes can use *without interacting with infrastructure entities*; *(ii)* it relies on the NDN Interest/Data primitives that are extended to guarantee privacy by using homomorphic encryption [9]. Thanks to this latter, NDN-P^2F performs calculations on encrypted forwarding metric values without decrypting them first, while maintaining low overhead and delays. As a result, forwarding decisions can be taken preserving the user's privacy.

II. Background

When considering privacy-preserving communications in ICN, solutions in the literature usually rely on encryption mechanisms and infrastructure elements that are responsible for the client's privacy [6]. In particular, the work in [7] leverages a brokering system that resolves encrypted queries from consumers and notifies a response with the route towards the desired provider. A tunneling-based protocol in [8] uses two proxies, one adjacent to the requester and another closer to the destination, to create two layers of encryption. The proposal in [10] supports the privacy with a name obfuscation mechanism established between consumers and producers, which does not require infrastructure support but needs a well-established and static route between the two endpoints.

These schemes cannot be straightforwardly applied in stand-alone wireless ad hoc scenarios. In this context, however, many existing forwarding protocols take decisions based on privacy-sensitive nodes' metrics (e.g., social centrality [5], geographical position [4]) sent in clear in NDN packets, thus potentially compromising the user's privacy.

Our proposal NDN-P^2F goes beyond existing works by providing a privacy-preserving forwarding scheme for NDN, where metrics are encrypted without affecting the effectiveness of the forwarding decision. To this purpose, it leverages the homomorphic encryption, a cryptographic system that allows computations on ciphertexts and generates encrypted results that, when decrypted, match the results of the operations as if they had been performed on plaintexts [9].

There are many homomorphic cryptosystems [9]. Here, we use the Paillier cryptosystem [11], because it is lightweight and, among its properties, it includes the homomorphic addition and multiplication of plaintexts and the homomorphic multiplication by a scalar. More specifically, the cryptographic homomorphic encryption function $E_k()$ satisfies the following properties for every constant a, b, and c value:

$$\begin{aligned} E_k(a) + E_k(b) &= E_k(a+b) \\ E_k(a) - E_k(b) &= E_k(a-b) \\ c \times E_k(a) &= E_k(c \times a) \end{aligned} \tag{1}$$

The Paillier cryptosystem does not provide a way of calculating the encrypted subtraction, but we use a mapping scheme proposed in [12] to be able to operate with negative numbers.

III. NDN Privacy-Preserving Forwarding

We consider a wireless ad hoc network consisting of nodes implementing NDN over an access layer technology like IEEE 802.11. Nodes maintain the conventional NDN tables, i.e., Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB). Data retrieval is based on NDN packets, with Interests forwarded from a node n_i to a node n_j according to a decision logic that compares the values of their privacy-sensitive metrics, m_{n_i} and m_{n_j}. Different metrics and decision logics can be implemented , the only requirement is that metrics must be scalar values.

As common in wireless ad hoc networks, NDN-P^2F is based on a reactive content discovery phase that precedes the content delivery phase. During the first phase, the proposed privacy-preserving forwarding is applied until the consumer discovers the content provider. Then, the normal content delivery phase takes place, where the Data packets composing the content (e.g., a video) are retrieved over the discovered path through the Interest solicitation. In Fig. 1, an example of the packet exchange in NDN-P^2F is depicted.

A. Content Discovery Phase

The discovery phase in NDN-P^2F is a three-stage process that leverages new defined packets, named Int-disc and Data-ack, and applies homomorphic encryption to securely exchange the forwarding metric among nearby potential forwarders until a content provider is found.

Stage 1: Int-disc broadcasting. A node n_1, which has to retrieve certain content but does not have a route to that content in its FIB, broadcasts a modified Interest packet that we call *discovery Interest*, Int-disc. In addition to the standard header fields, like the content name (e.g., */video/clip*), Int-disc includes: the node's public key (Pub_{n_1}) and its metric m_{n_1} encrypted with this public key ($E_{Pub_{n_1}}(m_{n_1})$).

Stage 2: Data-ack broadcasting. Each one-hop neighbour n_i receiving Int-disc can play one of the following roles: *(i) data provider*, if it keeps a copy of the searched content in the CS; *(ii) aware forwarder*, if the CS matching fails and it maintains a route for that content name in the FIB; *(iii) blind forwarder*, otherwise. To mitigate the broadcast storm probability and limit collisions due to multiple replies from receiving nodes, NDN-P^2F gives higher response priority to providers, then, to aware forwarders and finally, to blind forwarders. These nodes, based on their potential role, respectively defer their responses using a random delay as follows:

$$\begin{aligned} T_{dataProvider} &= rand[0,W] \times DefSlot \\ T_{awareForwarder} &= (W + rand[0,W]) \times DefSlot \\ T_{blindForwarder} &= (2W + rand[0,W]) \times DefSlot \end{aligned} \tag{2}$$

where $DefSlot$ and W values depend on the underlying IEEE 802.11 protocol time parameters [3]: *DefSlot* is a fixed time interval equal to the distributed interframe space, W is an integer equal to the minimum contention window, and the $rand$ function returns a random integer between 0 and W.

Depending on its role (provider, aware/blind forwarder), the receiver performs the following actions:

- If n_i is a provider, there is no need to further forward the packet. As response, n_i can broadcast a standard Data packet, by only adding its node ID, i.e, the IEEE 802.11 Medium Access Control (MAC) address, as new field in the packet header. The other potential forwarders, overhearing the Data transmission, do not perform further actions and cancel their possible response.

- If n_i candidates itself as an *aware forwarder*, a second encryption is required to protect its privacy. Specifically, it encrypts the value of its metric, m_{n_i}, using n_1's public key ($E_{Pub_{n_1}}$), and computes the subtraction of the two encrypted values: $E_{Pub_{n_1}}(m_{n_1}) - E_{Pub_{n_1}}(m_{n_i})$. Then, n_i chooses a random value (*nonce*) and multiplies it by the previous subtraction expression. Because of the homomorphic properties in Eq. (1) of the chosen cryptosystem, this is equivalent to:

$$nonce \times (E_{Pub_{n_1}}(m_{n_1} - m_{n_i})) \tag{3}$$

Finally, node n_i broadcasts a packet that we call Data acknowledgement, Data-ack, containing the content name and the following additional information: its node ID, a boolean value AwareF set to true, indicating it is an aware forwarder, and the result from Eq. (3). Similarly to the previous case, if blind forwarders overhear the broadcast transmissions from aware forwarders, they do not perform further actions.

- If n_i candidates itself as a blind forwarder because of the FIB matching failure, it performs the same operations as the aware forwarders but sets the AwareF flag to false.

Stage 3: FIB update. Depending on the received responses, node n_1 can update the FIB. To distinguish between providers, aware and blind forwarders, the FIB entry is extended with an additional integer field called NextHopType.

- If a one-hop data provider(s) is available, n_1 includes a new entry in the FIB that binds the content name with the discovered provider's MAC address, as the outgoing interface, and sets NextHopType = 0.

- Vice versa, n_1 collects the DATA-ACK packet(s)[1] from aware or blind forwarders and decrypts them obtaining:

$$Res = nonce \times (m_{n_1} - m_{n_i}) \tag{4}$$

By checking whether the result Res from Eq. 4 is greater or smaller than 0, n_1 knows if m_{n_1} is bigger or smaller than m_{n_i} without actually knowing m_{n_i}. Therefore, depending on the specific forwarding logic, n_1 can identify as candidate forwarders all the nodes whose metrics are bigger (or lower) than its own metric. For instance, in the case of a centrality metric, the forwarding logic can select the nodes with $m_{n_i} > m_{n_1}$. When collecting the responses, n_1 builds a FIB entry including, per that content name, the list of discovered nodes' MAC addresses as outgoing interfaces and sets NEXTHOPTYPE = 1 or 2, if the next hop is, respectively, an aware or blind forwarder.

B. Content Delivery Phase

Once the FIB has been updated, node n_1 selects the next hop. A provider, if available, is selected with the highest priority; otherwise n_1 targets an aware forwarder or, finally, a blind forwarder. If more nodes can play the same role, n_1 randomly selects one of them. NDN-P^2F does not introduce an explicit confirmation message, n_1 simply starts the content delivery phase by sending Interests to the selected next hop node. Broadcasting is now replaced by unicast transmissions, thus largely limiting the burden on the processing power of the network nodes. If the next hop does not answer the request before the download is completed, e.g., due to mobility, n_1 can select another next hop from the FIB and, in case of failure, revert to Stage 1 of the discovery phase.

C. Security Threats and Analysis

In this section, we first enumerate the threats to the privacy of our proposed NDN-P^2F, and then we explain how secure our proposal is when facing these threats.

Threat 1: Traffic observation. A node e may try to break the privacy of two nodes, n_i and n_j, implementing NDN-P^2F, by intercepting their messages over the wireless channel in order to obtain their metrics, m_{n_i} and m_{n_j}. **Privacy analysis (PA):** By overhearing the INT-DISC or DATA-ACK messages, node e may intercept $E_{Pub_{n_i}}(m_{n_i})$ and $nonce \times (E_{Pub_{n_i}}(m_{n_i} - m_{n_j}))$, respectively. Without having n_i's private key, these values cannot be decrypted. The significance of this threat is correlated to the ability of e in finding n_i's private key in terms of its public key. With a key long enough, this cryptanalysis is highly time-consuming.

Threat 2: Malicious candidate forwarder. A malicious candidate for forwarding, node n_j, which implements NDN-P^2F, may try to break the privacy of n_i by obtaining its m_{n_i} metric from the INT-DISC packet. **PA:** Node n_j receives $E_{Pub_{n_i}}(m_{n_i})$ from the INT-DISC packet. In the same way as in Threat 1, without having n_i's private key, this value cannot be decrypted.

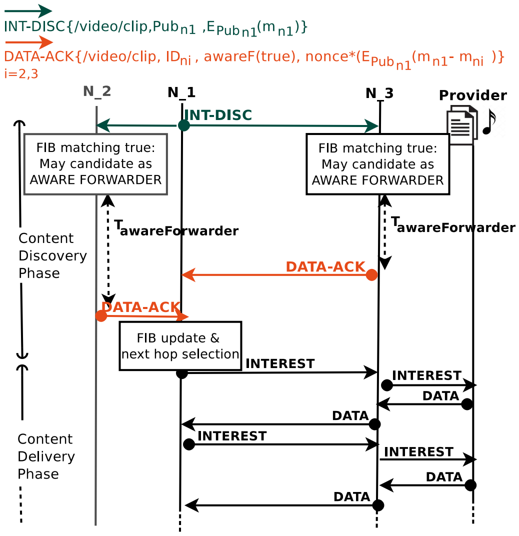
INT-DISC{/video/clip,Pub$_{n1}$,E$_{Pub_{n1}}$(m$_{n1}$)}
DATA-ACK{/video/clip, ID$_{ni}$, awareF(true), nonce*(E$_{Pub_{n1}}$(m$_{n1}$- m$_{ni}$)}
i=2,3
N_2
N_1
N_3
Provider
INT-DISC
FIB matching true: May candidate as AWARE FORWARDER
FIB matching true: May candidate as AWARE FORWARDER
T$_{awareForwarder}$
T$_{awareForwarder}$
Content Discovery Phase
DATA-ACK
DATA-ACK
FIB update & next hop selection
INTEREST
INTEREST
DATA
DATA
INTEREST
INTEREST
DATA
DATA
Content Delivery Phase

Fig. 1. Example of NDN-P^2F packets exchange: node n_1 broadcasts a INT-DISC packet, which is received by the neighbours n_2 and n_3. After receiving the DATA-ACKS, n_1 selects n_3 as forwarder.

Threat 3: Malicious forwarder. A malicious node n_i that implements NDN-P^2F may try to break the privacy of a next-hop node n_j by obtaining its m_{n_j} metric from the DATA-ACK packet. **PA:** The DATA-ACK packet sent by n_j contains the value Res according to Eq. (4). Node n_i is capable of decrypting this message, but it is not capable of inferring m_{n_j} because, even if n_i knows m_{n_i}, the expression is multiplied by an unknown $nonce$. Node n_i is capable of inferring whether m_{n_i} is greater or smaller than m_{n_j}, but not its value.

Threat 4: Malicious selected forwarder. A malicious forwarder, node n_j, which has been selected to forward an Interest packet by n_i, may try to break the privacy of n_i by obtaining m_{n_i}. **PA:** When node n_j is selected as next hop, it receives an Interest from n_i. The only information n_j can infer is the result of the forwarding decision.

IV. PERFORMANCE EVALUATION

The performance of NDN-P^2F is evaluated with ndnSIMv2.7 (http://ndnsim.net/). An 800m x 800m topology is simulated, where 100 mobile nodes, implementing NDN-P^2F over IEEE 802.11a in ad hoc mode, move according to the pedestrian Truncated Levy-Walk model [13], and a Road Side Entity (RSE) in the middle of the topology provides location-based contents. We consider a catalogue of 1000 distinct 100KB-large contents, divided into Data packets of 1000 bytes each. A variable number of nodes (from 10 to 40) request contents according to a Zipf distribution with the *skewness parameter* (α) varying from 0.4 (low popularity) to 2 (high popularity). Contents, originally owned by the RSE, can be retrieved in a multihop fashion and potentially cached by any mobile node during the simulation. The signal propagation is modelled through the Rayleigh distribution to account for wireless channel-induced losses.

[1] We assume that the collection time is equal to the maximum deferral time plus a fixed single hop round-trip time.

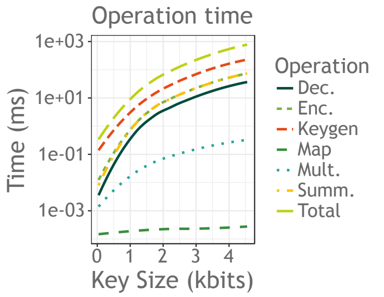

Fig. 2. Arithmetic operation time as a function of the homomorphic key size.

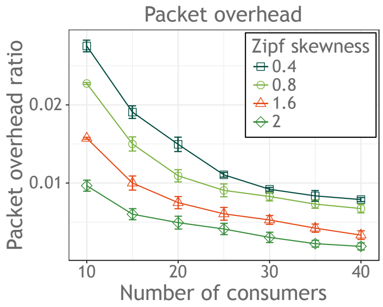

Fig. 3. Packet overhead ratio.

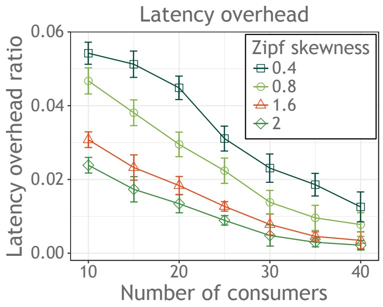

Fig. 4. Latency overhead ratio.

The evaluation has two main targets. First, it quantifies the *processing delay* due to the homomorphic encryption; second, it identifies the *overhead* cost of preserving privacy in NDN-P^2F when compared to a non-privacy preserving protocol, in the following referred to as “non-PRIV”.

For both protocols, we consider a simple *distance-based* forwarding decision logic that leverages as reference the position of the RSE, known by the mobile nodes. In non-PRIV, a consumer does not use the INT-DISC/DATA-ACK signalling packets and piggybacks its distance from the RSE as clear text in the Interest. Each receiving node, which is closer to the RSE than the sender, can act as a forwarder. In NDN-P^2F, the distance metric is instead encrypted and carried in the INT-DISC/DATA-ACK packets.

Simulation results are averaged over 20 independent runs and reported with the 95% confidence intervals. Each run ends when all the consumers have retrieved the requested content.

Figure 2 shows the processing delay due to the arithmetical and cryptographic operations needed to implement NDN-P^2F, as a function of the cryptographic homomorphic key size. A key size of 512 bits gives a good trade-off between security and performance; in this case, in fact, the operations of encryption and decryption are not time-consuming (0.1ms and 0.05ms, respectively). Based on this result, in the following simulations, we consider a key of 512 bits.

Two overhead metrics are considered to capture the cost of NDN-P^2F. The *packet overhead ratio* measures the cost in terms of additional signalling packets used by NDN-P^2F. It is computed as the difference between the total number of NDN-P^2F packets (INT-DISC/DATA-ACK, Interest/Data) and the total number of non-PRIV packets (Interest/Data), transmitted during the simulation by all the nodes involved in the content retrieval, over the total number of non-PRIV packets.

The *latency overhead ratio* is computed as the difference between the average time required for a consumer to retrieve the desired content with NDN-P^2F and the same time obtained with non-PRIV, over the time obtained with non-PRIV.

Results in Fig. 3 show that the packet overhead introduced by NDN-P^2F is very limited, and it decreases when the number of consumers and the Zipf skewness parameter increase, going from less than 3%, in the worst case, to less than 0.2% in the best case. Consequently, the latency overhead in Fig. 4 also decreases following a similar trend. This occurs because a consumer has a higher probability to find a cached content copy in a close node when the number of consumers and the skewness parameter increase, and therefore less signalling packets and encryption/decryption operations are required.

V. CONCLUSIONS

In this letter, we proposed a privacy-preserving homomorphic encryption-based forwarding scheme for ad hoc ICN. It can be easily applied to distinct ICN forwarding protocols that take as input users’ personal information. Simulations have shown that the overhead produced by our scheme is very low.

REFERENCES

[1] G. Xylomenos *et al.*, “A survey of information-centric networking research.” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 2, pp. 1024–1049, 2014.

[2] L. Zhang *et al.*, “Named data networking,” *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[3] X. Liu *et al.*, “Information-centric mobile ad hoc networks and content routing: a survey,” *Ad Hoc Networks*, vol. 58, pp. 255–268, 2017.

[4] G. Grassi *et al.*, “VANET via named data networking,” in *INFOCOM Workshops*, 2014, pp. 410–415.

[5] Y. Lu, X. Li, Y.-T. Yu, and M. Gerla, “Information-centric delay-tolerant mobile ad-hoc networks,” in *2014 IEEE conference on Computer communications workshops (INFOCOM WKSHPS)*, 2014, pp. 428–433.

[6] R. Tourani, S. Misra, T. Mick, and G. Panwar, “Security, privacy, and access control in information-centric networking: A survey,” *IEEE communications surveys & tutorials*, vol. 20, no. 1, pp. 566–600, 2018.

[7] N. Fotiou *et al.*, “Enhancing information lookup privacy through homomorphic encryption,” *Security and Communication Networks*, vol. 7, no. 12, pp. 2804–2814, 2014.

[8] S. DiBenedetto *et al.*, “Andana: Anonymous named data networking application,” *arXiv preprint arXiv:1112.2205*, 2011.

[9] C. Fontaine and F. Galand, “A survey of homomorphic encryption for nonspecialists,” *EURASIP Journal on Information Security*, vol. 2007, no. 1, pp. 1–10, 2007.

[10] S. Arianfar *et al.*, “On preserving privacy in content-oriented networks,” in *Proceedings of the ACM SIGCOMM workshop on Information-centric networking*, 2011, pp. 19–24.

[11] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *EUROCRYPT*. Springer, 1999, pp. 223–238.

[12] A. Sanchez *et al.*, “Privhab: A privacy preserving georouting protocol based on a multiagent system for podcast distribution on disconnected areas,” *Ad Hoc Networks*, vol. 53, pp. 110–122, 2016.

[13] I. Rhee *et al.*, “On the levy-walk nature of human mobility,” *IEEE/ACM transactions on networking (TON)*, vol. 19, no. 3, pp. 630–643, 2011.