ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

# Creating Secrets Out of Packet Erasures

Sheetal Modke, Prof. Pradnya Kasture

M.E, Dept. of Computer, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, Maharashtra, India.

Professor, Dept. of Computer, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, Maharashtra, India

**ABSTRACT:** We develop protocols for making pair wise secrets between nodes in an exceedingly wireless network,, so that these secrets are secure from an eavesdropper, Eve, with unbounded computational and memory capabilities, but with limited network presence. We first present a basic secret-agreement protocol for single-hop networks, where secrets are constructed using traffic exchanged between the nodes, and we show that under standard theoretical assumptions, our protocol is information-theoretically secure. Second, we propose a secret-agreement protocol for arbitrary, multi-hop networks that build on the basic protocol but also comprises design features for leveraging additional sources, that multi-hop offers, for secrecy. Finally, we evaluate our protocols, and we provide experimental evidence that it is feasible to create thousands of secret bits per second, in realistic wireless setups, the security of which is independent of Eve's computational capabilities.

**KEYWORDS:** Secret key generation, packet erasures, multi-hop key agreement, wireless networks.

## 1. INTRODUCTION

In recent years, there has been significant interest on building information theoretical security out of wireless channel properties, but the work has been limited to very specific topologies and scenario. The majority of the work considers pair wise key generation over a single channel with a single source and receiver, (see also and references therein); the few works that have looked at multiple receivers still only consider a single source and receivers within the same broadcast. Works that look at larger networks typically do not provide strong, but weak information security guarantees, and mostly focus on single message distribution, as opposed to creating n 2 different secret keys (see also Section VIII on related work). Moreover, in most of the proposed practical works, the secret key generation rates achieved are only a few tens of bits per second. In contrast, we show in this paper that can we leverage both channel and network properties, to create pair wise keys at rates that are of the order of Kb per second, for arbitrary n and wireless network topologies.

Our main contributions in the paper are as follows: First, we present a basic secret-agreement protocol, which enables n nodes connected to the same broadcast domain to create pair wise secrets that Eve knows very little about. Our protocol leverages the broadcast nature of the wireless to create pair wise secrets between all pair of nodes simultaneously, has polynomial time complexity and is readily implementable in simple wireless devices. We analyze our protocol in two ways: (i) under standard information-theory assumptions (independent erasure channels between nodes and known erasure probabilities), we formally show that: (1) our basic protocol is information-theoretically secure, i.e., it leaks no information to Eve about the secrets. (2) It achieves a secret generation rate that is optimal for n = 2 nodes and scales well with the number of nodes n. (ii) through experimental evaluation, and estimation of the network parameters, as we discuss later. Second, we consider secret-agreement over arbitrary, multichip networks. This is important, firstly, from a practical point of view: even when networks have a small number of nodes, as connectivity is impaired from distance, interference and other impediments (e.g., metal obstructions), it is challenging to consistently maintain a single-hop connected network. Secondly, multi-hop networks are also interesting from a technical point of view since they provide two new opportunities for secrecy that we could leverage: interference and multi-path propagation. Interference between concurrent transmissions (such as caused by the hidden terminal problem) may interfere with Eve's reception but not with the reception of other legitimate nodes; distinct packet propagation through multiple paths can ensure that Eve, located in an unknown but fixed position in our network, does not have access to all of them, and again misses packets that legitimate nodes receive. Finally, secret-agreement over arbitrary multi-hop networks can enable applications similar to the one we proposed. Third, we experimentally evaluate the performance of our protocols and we provide evidence that it is feasible in practice to create pair wise secrets at rates of thousands of bits per second in realistic setups. In the experimental setup, we assume no knowledge of channel parameters, and no knowledge of Eve's location or collected information – we estimate the quantities we need online. For the single-hop case, we use a small wireless tested and for the multi-hop case we simulate different network configurations, consisting of up to 500 nodes and located up to 5-hops apart. We show that we can achieve secret generation rates in the magnitude of Kbps, independently from the adversary's computational capabilities. In summary, our contributions in this paper are: 1) We design practical secret-agreement protocols for simultaneously generating n 2 secrets in: a) single-hop networks, by leveraging channel properties, b) arbitrary multi-hop networks, by leveraging both channel and network properties. 2) We evaluate the performance of our protocols through experimentation in realistic wireless environments. We note that the secret-agreement protocol for single-hop networks and a subset of the single-hop experimental results have been initially presented in our conference paper. In particular, we demonstrated the minimum achievable secrecy rates in our tested, whereas here we present more generalized measurements that lead to new observations on secret key generation in a real wireless network. Extending the work to multi-hop networks is not a straightforward step, as new challenges, but also new opportunities, arise: we need to design a custom dissemination protocol, and we need to leverage additional sources of secrecy, in addition to channel noise. The multi-hop protocol and the associated experimental results are presented here for the first time.

## II. LITERATURE SURVEY

Proposed new approach for secret key extraction where multiple sensors collaborate in exchanging probe packets and collecting channel measurements. Essentially, measurements from multiple channels have substantially higher differential entropy compared to the measurements from a single channel, thereby resulting in more randomness in the information source for key extraction, and this in turn produces stronger secret keys. We also explore the fundamental trade-off between the quadratic increase in the number of measurements of the channels due to multiple nodes per group versus a linear reduction in the sampling rate and a linear increase in the time gap between bidirectional measurements [1].

Evaluate a traffic anonymization protocol for wireless networks, aiming to protect against computationally powerful adversaries. Our protocol builds on recent key-generation techniques that leverage intrinsic properties of the wireless together with standard coding techniques. We show how to exploit the security properties of such keys to design a Tarlike anonymity network, without making any assumptions about the computational capabilities of an adversary [2].

Propose a simple secret-agreement protocol, where the wireless nodes keep exchanging bits until they have agreed on pair wise secrets that Eve cannot reconstruct with very high probability. Our protocol relies on Eve's limited network presence (the fact that she cannot be located at an arbitrary number of points in the network at the same time), but assumes nothing about her computational capabilities. We formally show that, under standard theoretical assumptions, our protocol is information-theoretically secure (it leaks zero information to Eve about the secrets) [3].

Current security systems typically rely on the adversary's computational limitations (e.g., the fact that it cannot invert a hash function or perform large-integer factorization). Wireless networks offer the opportunity for a different, complementary kind of security, which relies not on the adversary's computational limitations, but on its limited network presence (i.e., that the adversary cannot be located at many different points in the network at the same time). We take a first step toward designing and building a wireless security system that leverages this opportunity: We consider the problem where a group of n nodes, connected to the same broadcast wireless network, want to agree on a shared secret (e.g., an encryption key), in the presence of an adversary Eve who tries to listen in and steal the secret. We propose a secret-agreement protocol, where the n nodes of the group keep exchanging bits until they have all agreed on a bit sequence that Eve cannot reconstruct (with very high probability) [4].

Propose a model; call the wiretap network that incorporates information security with network coding. In this model, a collection of subsets of the channels in the network is given, and a wire tapper is allowed to access any one (but not more than one) of these subsets without being able to obtain any information about the message transmitted. Our model includes secret sharing in classical cryptography as a special case. We present a construction of secure linear network codes that can be used provided a certain graph-theoretic condition is satisfied. We also prove the necessity of this condition for the special case that the wire tapper may choose to access any subset of channels of a fixed size. The optimality of our code construction is established for this special case [5].

Provide a synopsis of the state of the art in coding for secrecy. We discuss the general principles of coding, and we illustrate them with several examples. In particular, we discuss the importance of a nested code structure and stochastic encoding, which allow for both data reliability and security. Introduction Confidentiality has traditionally been addressed at higher layers of communications systems using cryptographic protocols. With the advent of the Internet and wireless networks, data confidentiality has become a growing concern, and techniques have been developed at lower layers in the protocol stack as well. Arguably, the last layer included in the security effort has been the physical layer. The idea of exploiting the imperfections of the physical layer as a first layer of defense has recently attracted much interest and is now colloquially known as physical-layer security [6].

Current security systems often rely on the adversary's computational limitations. Wireless networks offer the opportunity for a different, complementary kind of security, which relies on the adversary's limited network presence (i.e., that the adversary cannot be located at many different points in the network at the same time). We present a system that leverages this opportunity to enable n wireless nodes to create a shared secret S, in a way that an eavesdropper, Eve, obtains very little information on S. Our system consists of two steps: (1) The nodes transmit packets following a special pattern, such that Eve learns very little about a given fraction of the transmitted packets. This is achieved through a combination of beam forming (from many different sources) and wiretap codes. (2) The nodes participate in a protocol that reshuffles the information known to each node, such that the nodes end up sharing a secret that Eve knows very little about. Our protocol is easily implementable in existing wireless devices and scales well with the number of nodes; these properties are achieved through a combination of public feedback, broadcasting, and network coding. We evaluate our system through a 5-node testbed. We demonstrate that a group of wireless nodes can generate thousands of new shared secret bits per second, with their secrecy being independent of the adversary's computational capabilities. [7]

## III. PROBLEM STATEMENT AND OBJECTIVE

### 3.1Problem Statement

The problem where a group of n wireless nodes that form an ad-hoc wireless network, want to create n 2 pair wise secrets, such that a passive eavesdropper Eve, who is located in an unknown position in the network, learns very little about them. Current cryptographic secret agreement algorithms are designed around computational hardness assumptions: security breach cannot be achieved in useful time, since Eve does not possess sufficient computational power. We are interested instead in strong information theoretical or unconditional security, where security does not depend on computational limitations of Eve, but rather on the fact that Eve does not possess enough information to breach security. We are asking, whether it is possible to offer strong security, as the number of nodes n and number of pair wise keys increases, and over arbitrary wireless topologies.

### 3.2Objective

We propose a secret-agreement protocol for multi-hop networks that builds on our basic protocol, but also comprises new design features that realize the benefits multi-hop offers for secrecy. This includes a customized packet dissemination protocol that balances two conflicting goals: spreading the packets as efficiently and as widely as

possible among the legitimate nodes, while ensuring that a significant fraction of packets will not be overheard by Eve, who could be located in any place within the network. Our protocol is completely decentralized, does not differentiate between nodes and is readily implementable in simple wireless devices.
Scope is to investigate further the robustness of our protocols, under the presence of adversaries with increasing network presence (multiple antennas, collaborating Eves etc.).

## IV. METHODOLOGY

### 1. BASIC SECRET-AGREEMENT PROTOCOL

In this section, we describe the core of our secret-agreement protocol, that enables terminals Ti and Tj , which are connected in the same broadcast domain, i.e., they form a single-hop network, to create a secret $S_{ij}$ . Assuming the theoretical network conditions, $S_{ij}$ is perfectly secret from any terminal $Tk\neq i,j$ and an adversary Eve .

### 2. SECRET-AGREEMENT FOR MULTI-HOP NETWORKS

In this section we describe a secret-agreement protocol for multi-hop networks that builds on the basic protocol and comprises new design features. In addition to channel noise and fading, multi-hop networks offer two more sources of packet erasures, that we aim to exploit for creating secrets: (1) interference from simultaneous transmissions, (2) existence of multiple paths between terminals. We design a protocol, consisting of a packet dissemination phase followed by a feedback phase that essentially replaces the initial phase of the basic secret-agreement protocol.

## V. ALGORITHMS

### Algorithm 1

Each terminal $T_i$ maintains $n - 1$ queues $Q_{ij}$, $j \neq i$. In the beginning, these are empty.

### Initial Phase

In round $r = 1 \ldots n$:

1) Terminal $T_r$ generates and transmits N random packets (we will call them x-packets).

2) Each terminal $T_i \neq r$ reliably broadcasts the identifiers of the x-packets it received.

3) Each terminal $T_i$ adds to queue $Q_{ij}$ the identifiers and contents of the x-packets it shares with terminal $T_{j\neq i}$.

At this point, $Q_{ij}$ contains all the packets shared by terminals $T_i$ and $T_j$ .

### Privacy Amplification Phase

For $i = 1 \ldots n - 1$:

1) Terminal $T_i$ constructs $M_{ij}$ linear combinations of the packets in the queue $Q_{ij}$ , for all $j > i$ (we will call them y-packets).

It determines the number of y-packets $M_{ij}$ and constructs the y-packets.

2) Terminal $T_i$ reliably broadcasts the coefficients it used to construct the y-packets.

3) Each terminal $T_{j>i}$uses the broadcasted coefficients and the contents of its queue $Q_{ij}$ to reconstruct the $M_{ij}$ y-packets.

DOI: 10.15680/IJIRCCE.2018.0604094

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

At this point, terminals $T_i$ and $T_{j>i}$ share $M_{ij}$ y-packets. Their secret $S_{ij}$ is the concatenation of these y-packets.

**Algorithm 2**

**1. Additional Parameters and Notation:**

Each terminal $T_i$ can generate x-packets but also forward the x-packets generated by any other terminal in the network. In the unique identifier of each generated x-packet, a field ttl is appended describing the maximum number of times this packet can be transmitted in the network. Whenever a terminal transmits an x-packet (either generated locally or received by another terminal) is referred to as the sender of this packet. Each terminal transmits at rate $\frac{1}{\lambda}$, where λ is the number of its neighbors.

**2. Packet Dissemination Phase:**

Each terminal $T_i$ maintains $n - 1$ queues $Q_{ij}$ , $j \neq i$, that are empty in the beginning, and it records all overheard traffic. The packet dissemination is performed as follows:

1) Each terminal $T_i$ generates and transmits N x-packets; it waits a random time between transmissions so that on average it transmits at rate $\frac{1}{\lambda}$ .

2) Upon reception of an x-packet p, the receiver checks if this is first time it received this packet; if yes, the receiver unicasts an acknowledgment to the sender, otherwise it does not acknowledge.

3) The sender of a packet p selects a forwarder: Let $R_p$ denote the set of terminals that acknowledged p. The sender chooses a terminal uniformly at random from $R_p$, and unicasts a control message to inform the node it is the selected forwarder. If $R_p = \emptyset$, then p is not forwarded anymore.

4) The selected forwarder of a packet p (the next sender of p), reduces the ttl field by one and transmits it. Steps 2 to 4 are repeated till the ttl field of all the packets in the network expires. Note that when transmitting a packet p the sender sets a timer $T_p$, which defines a time window for acknowledging. Once $T_p$ has expired, step 3 takes place.

**3) Feedback Phase**:

For i = 1 ... n:

1) $T_i$ constructs a 1×nN vector $v_i$ , with a "1" in the jm$^{th}$ position if $T_i$ has received the packet with sequence number m from terminal $T_j$ , and a "0" otherwise.

2) $T_i$ reliably broadcasts $v_i$ into the network, using special packets indicated as feedback packets.

3) Each terminal $T_j$ adds to queue $Q_{ij}$ the identities and contents of the x-packets it shares with terminal $T_{i \neq j}$ .

**4) Privacy Amplification Phase:**

The terminals perform the privacy amplification phase as described in Sections III-B and III-E. Each pair of terminals $T_i/T_j$ can construct up to $M_{ij}$ y-packets, the concatenation of which is their common secret $S_{ij}$. Regarding the value of variable $V_E$ .

DOI: 10.15680/IJIRCCE.2018.0604094

## V. CONCLUSION

We have presented two protocols for enabling a group of n wireless nodes to create pair wise secrets, in the presence of a passive adversary, with limited network presence, without assuming anything about her computational and memory capabilities. Our basic secret-agreement protocol operates in single-hop networks, it is information-theoretically secure and leverages broadcast to create secrets simultaneously between all terminal pairs. A main assumption we do is that Eve is a passive adversary. In the case that Eve is an active adversary (tries to impersonate a terminal), the terminals need to share some bootstrap information to authenticate each other when they first communicate. The need for this bootstrap information is fundamentally unavoidable: without it, there is no way for Alice to know she is talking to Bob until they have established their first secret. Authentication is orthogonal to our secret agreement and can happen in different ways, e.g., by requiring the terminals to initially share bootstrap information and use it to construct authentication codes for the x-packets (and the feedback packets) they transmit the first time they run our protocols. After the terminals have established their first pair wise secrets using our protocols, they can use these to construct new authentication codes, which do not depend on the bootstrap information. The advantage of our protocols is that they enable the terminals to keep generating new secrets, independent from the previous ones, and continuously refresh their encryption and authentication keys. Unless the adversary can break into one of the terminals while they run our protocols, she has a small window of opportunity to compromise their communication: she has to steal the bootstrap information and impersonate a terminal while the terminals are running our protocols for the first time.

## REFERENCES

[1] S. N. Premnath, J. Croft, N. Patwari, and S. K. Kasera, “Efficient highrate secret key extraction in wireless sensor networks using collaboration,” ACM Trans. Sensor Netw., vol. 11, no. 1, 2014, Art. ID 2.

[2] I. Safaka, L. Czap, K. Argyraki, and C. Fragouli, “Towards unconditional Tor-like anonymity,” in Proc. Int. Symp. Netw.Coding (NetCod), 2015, pp. 66–70.

[3] I. Safaka, C. Fragouli, K. Argyraki, and S. Diggavi, “Exchanging pairwise secrets efficiently,” in Proc. IEEE INFOCOM, Apr. 2013, pp. 2265–2273.

[4] I. Safaka, C. Fragouli, K. Argyraki, and S. Diggavi, “Creating shared secrets out of thin air,” in Proc. 11th ACM Workshop Hot Topics Netw., 2012, pp. 73–78.

[5] N. Cai and R. W. Yeung, “Secure network coding on a wiretap network,” IEEE Trans. Inf. Theory, vol. 57, no. 1, pp. 424–435, Jan. 2011

[6] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, “Coding for secrecy: An overview of error-control coding techniques for physical-layer security,” IEEE Signal Process. Mag., vol. 30, no. 5, pp. 41–50, Sep. 2013.

DOI: 10.15680/IJIRCCE.2018.0604094