UNIVERSITY
OF TRENTO

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

38050 Povo – Trento (Italy), Via Sommarive 14
http://www.dit.unitn.it

HIERARCHIAL SECRET SHARING IN AD HOC NETWORKS THROUGH BIRKHOFF INTERPOLATION

E. Ballico, G. Boato, C. Fontanari, and F. Granelli

July 2005

Technical Report DIT-04-080

Hierarchical Secret Sharing in Ad Hoc Networks through Birkhoff Interpolation

E. Ballico[1], G. Boato[2], C. Fontanari[1], and F. Granelli[2]
[1]Dept. of Mathematics, [2]Dept. of Information and Communication Technology
University of Trento
Via Sommarive 14, I-38050 Trento (Italy)
{ballico, fontanar}@science.unitn.it, {boato, granelli}@dit.unitn.it

Abstract

Securing ad hoc networks represents a challenging issue, related to their very characteristics of decentralized architecture, low-complexity, and multiple hops communications. Even if several methods are available, this paper presents a novel approach to allow secret sharing of information at lower levels of the node protocol stack. In fact, secret sharing schemes provide a natural way of addressing security issues in ad hoc networks. To this aim, a flexible framework for secure end-to-end transmission of confidential information is proposed which exploits multipath source routing and hierarchical shares distribution. Such a goal is achieved by designing an ideal, perfect, and eventually verifiable secret sharing scheme based on Birkhoff polynomial interpolation and by establishing suitable hierarchies among independent paths.

I. Introduction

Nowadays, ad hoc networks represent a relevant research topic in the field of telecommunication networks. In an ad hoc network wireless hosts communicate with each other in the absence of a fixed infrastructure. They can be used in several applications, ranging from tactical operations, to establish quickly military communications during the deployment of forces in unknown and hostile terrain, to rescue missions, for communication in areas without adequate wireless coverage; from exhibitions or conferences or virtual classrooms, to sensor networks, for communication between intelligent sensors. A wireless ad hoc network presents a larger spectrum of security problems than conventional wired and wireless networks, due to the broadcast nature of the transmission medium and vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. As in any wireless environment, the nodes are easy to capture, compromise and hijack. An attacker can listen to and modify all the traffic on the wireless communication channel, and may attempt to masquerade as one of the participants. Due to the absence of any central support infrastructure, authentication based on public key cryptography and certification authorities may be difficult to accomplish.

There has been a flurry of research and development effort in the field of security in ad hoc networks, but results are still incomplete. Due to the severe hardware and energy constraints, selecting appropriate cryptographic primitives and security protocols in ad hoc networks is a problematic point. A usual approach for keeping sensitive

This research is partially funded by the T.A.S.C.A. project of I.N.d.A.M., supported by P.A.T. (Trento) and M.I.U.R. (Italy), and by the DIPLODOC project, funded by P.A.T. (Trento).

data secret is to encrypt the data with a secret key known also by the receiver, ensuring in this way confidentiality. As already said, the general energy contraint in these networks creates limits also for security, due to consumption of processor power. Moreover, in asymmetric cryptographic algorithms (used for example in Encapsulating Security Payload to provide confidentiality in IPSec ([1])) the length of keys which provide security is often too high for node's working memory. To achieve confidentiality means to prevent intermediate or non-trusted nodes from understanding the contents of packets. A lot of protocols offer solutions using cryptographic algorithms (see [2], [3], [4]).

The idea of the paper is to exploit the specific characteristics of an ad hoc network (multihop data delivery, absence of fixed infrastructure, decentralized architecture) in order to enforce security at the lower levels of the protocol stack (i.e., MAC layer). In particular, we propose a method to achieve end-to-end data protection against passive attacks in ad hoc networks where the nodes are not highly mobile. We focus on a method which permits to achieve confidentiality exploiting multiple paths between source and destination and taking into account different characteristics of the paths. As a consequence, the next paragraphs are focused on *secret sharing schemes*. A method which exploits multiple paths avoiding message retransmission is to transmit redundant information through additional routes for error detection and correction [5]: part of the disjoint routes are used to transmit data and part for redundant information. In such a way if certain routes are compromised, the receiver is able to recover the message. In our method the transmission exploits multiple paths but improving the concept of redundant information. In the previous example confidentiality can be achieved only by adding encryption. We pretend to avoid the use of cryptographic algorithms for the already mentioned reasons. The key point of our scheme is that a non-trusted node intercepting a packet gets no information about the transmitted data. This is achieved with a secret sharing scheme. In [5], the usage of threshold schemes for key management is proposed. The same principle together with multipath routing is exploited, also in the case of data transmission, in [6]. A (k, n) threshold sharing scheme allows to divide a confidential message into n shares and requires the knowledge of at least k out of n shares to reconstruct the original content. Each share does not carry any meaningful partial plaintext of the original message and, if the number of shares available is less than k, a potential attacker can do no better than guessing, even with infinite computing time and power. The basic scheme, due to Shamir ([7]), relies on standard Lagrange polynomial interpolation and introduces a hierarchical approach by simply assigning a higher number of shares to higher level (more important, or reliable) participants. More recently, a refined hierarchical scheme was obtained by Tassa ([8]) from subtler properties of Birkhoff polynomial interpolation.

In order to exploit different characteristics of paths and in particular different trust levels, it is natural to apply a hierarchical model. For instance, the protocol SAR (Security Aware Ad Hoc Routing) proposes the Quality of Protection bit vector to classify routes [3]. Even though a hierarchical secret sharing scheme seems to be suitable also for an ad hoc network, nevertheless the previous approaches suffer from severe constraints for practical implementation. Namely, efficiency of Shamir's proposal is compromised by the systematical delay due to multiple assignments. On the other hand, Tassa's algorithm works only on large finite fields (see [8], Theorem 4), making it unsuitable for an ad hoc node with limited computational resources.

In order to overcome such difficulties, the present paper introduces an alternative scheme for secure information sharing in ad hoc networks applications. As in Tassa's approach, Birkhoff interpolation theory is applied, but with some crucial improvements. In particular, random allocation of participants enables to exploit stronger mathematical tools and drastically reduce the size of the base field. Furthermore, each participant receives only one share

(overcoming the main drawback of Shamir's hierarchical scheme) and the secret is identified with a sequence of elements of the field (reflecting the natural structure of a message as a sequence of packets). As a consequence, both the delay and the overhead are significantly reduced.

The structure of the paper is the following. In Section II, after recalling the definition of hierarchical secret sharing, the proposed sharing scheme is introduced and a mathematical proof that it is ideal, perfect, and eventually verifiable is given. In Sections III and IV, a hierarchical multipath framework for ad hoc networks is described, providing both a general scheme and a sample application scenario. Finally, in Section V, some concluding remarks and outlines about future work on the topic are presented.

II. Description and Analysis of the Proposed Algorithm

The basic scheme proposed by Shamir [7] relies on standard Lagrange polynomial interpolation. To be explicit, Shamir's idea is simply to identify a secret $S \in \mathbb{R}$ with some coefficient of a polynomial

$$p(x) = \sum_{i=0}^{k-1} a_i x^i$$

where for instance $a_0 = S$ and $a_1, \ldots, a_{k-1}$ are arbitrary real numbers. In order to distribute S among n participants, just fix n distinct real numbers $v_1, \ldots, v_n$ and assign to the j-th participant the share

$$p(v_j) = \sum_{i=0}^{k-1} a_i v_j^i$$

In order to reconstruct the secret, a subset of participants with associated real numbers $\{v_{i_1}, \ldots, v_{i_s}\}$, with $1 \leq i_1 < i_2 < \ldots < i_s \leq n$, has to solve the following linear system:

$$A \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} p(v_{i_1}) \\ \vdots \\ p(v_{i_s}) \end{pmatrix} \tag{1}$$

where

$$A = \begin{pmatrix} 1 & v_{i_1} & \ldots & v_{i_1}^{k-1} \\ \vdots & & & \vdots \\ 1 & v_{i_s} & \ldots & v_{i_s}^{k-1} \end{pmatrix}$$

is a so-called *Vandermonde matrix*. It follows that the linear system (1) admits a unique solution if and only if $s \geq k$. In particular, at least k out of n shares are needed to reconstruct S, hence we obtain a (k, n) secret sharing scheme.

As pointed out by Shamir himself in [7], a hierarchical variant can be introduced by simply assigning a higher number of shares to higher level participants. More recently, a refined hierarchical scheme was obtained by Tassa [8] from subtler properties of Birkhoff polynomial interpolation.

Let U be a given set of n participants and fix a collection Γ of subsets of U, which is monotone in the sense that if $I \in \Gamma$ then any set containing I also belongs to Γ. A threshold secret sharing scheme with *access structure* Γ is a method of sharing a secret among the members of U, in such a way that only subsets in Γ can recover the secret, while all other subsets have no information about it. Assume that U is divided into levels, i.e. $U = \cup_{l=0}^{t} U_l$ with $U_i \cap U_j = \emptyset$ for every $i \neq j$. If $0 < k_0 < \ldots < k_t$ is a strictly increasing sequence of integers, then a

$(k_0, \ldots, k_t; n)$ hierarchical threshold secret sharing scheme distributes to each participant a share of a given secret S, in such a way that

$$\Gamma = \left\{ V \subset U : \#V \cap \left(\cup_{l=0}^{i} U_l \right) \geq k_i \quad \forall i = 0, \ldots, t \right\}$$

where $\#$ states cardinality.

Roughly speaking, a subset of participants can reconstruct the secret if and only if it contains at least k_0 members of level 0, at least k_1 members of level 0 or level 1, at least k_2 members from levels 0, 1, and 2, and so on.

In order to construct a suitable $(k_0, \ldots, k_t; n)$ hierarchical threshold secret sharing scheme, it is natural to apply Birkhoff interpolation instead of Lagrange interpolation. The key point is that the Birkhoff scheme involves not only a polynomial, but also its (higher order) derivatives. To be formal, as in [11], p. 124, let $E = (E_{i,j})$, $i = 1, \ldots, m$; $j = 0, \ldots, k-1$, be an $m \times k$ *interpolation matrix*, whose elements are zeros or ones, with exactly k ones. Let $X = x_1, \ldots, x_m$, $x_1 < x_2 < \ldots < x_m$, be a set of m distinct *interpolation points*. For polynomials

$$p(x) = \sum_{i=0}^{k-1} a_i x^i$$

of degree $\leq k-1$ we consider the k interpolation equations

$$p^{(j)}(x_i) = B_{i,j}$$

for $E_{i,j} = 1$, where $p^{(j)}$ denotes the j-th derivative of p and $B_{i,j}$ are given data. Here the unknowns are the k coefficients $a_0, \ldots, a_{k-1}$ of $p(x)$. However, it is easy to convince ourselves that a Birkhoff interpolation problem can admit infinitely many solutions even if the number of equations equals the number of unknowns. Indeed, think for a moment at the case in which $E_{i,0} = 0$ for every $i = 1, \ldots, m$. In such a case, the interpolation system involves only derivatives of the polynomial p, hence it keeps no track of the constant term a_0, which remains undetermined. More generally, elementary linear algebra considerations show that if a Birkhoff interpolation problem admits a unique solution then its associated interpolation matrix $E = (E_{i,j})$, $i = 1, \ldots, k$; $j = 0, \ldots, k-1$, has to satisfy the following *Pólya condition*

$$\#\{E_{i,j} = 1 : j \leq h\} \geq h+1 \quad 0 \leq h \leq k-1$$

(see for instance p. 126 of [11]).

The idea now is to exploit this necessary condition in order to ensure that only authorized subsets can reconstruct the secret. Intuitively speaking, an evaluation of the polynomial itself carries more informations than an evaluation of any of its derivatives since it involves more coefficients; therefore it sounds reasonable to assign to a participant of higher level the evaluation of a lower order derivative.

For shares generation, we propose the following algorithm:

1) Select a finite field $\mathbb{F}$ with characteristic $p \geq k$ and cardinality $q \geq \frac{k_t(k_t-1)}{2}$. Identify the secret S with a sequence $(S_0, \ldots, S_z)$ with $0 \leq z \leq k_t - 1$ and $S_i \in \mathbb{F}$ for every i.
2) Let $k = k_t$ and pick a polynomial
$$p(x) = \sum_{i=0}^{k-1} a_i x^i$$
where $a_i = S_i$ for every $0 \leq i \leq z$ and a_i arbitrary elements of $\mathbb{F}$ for $z+1 \leq i \leq k-1$.
3) Identify each participant of level l with a random element $u \in \mathbb{F}$ and associate to u the share $p^{(k_{l-1})}(u)$, where $p^{(h)}$ denotes the h-th derivative of p and $k_{-1} := 0$.

We stress that for $z = 0$ our scheme is *ideal*, i.e. the size of the shares is equal to the size of the secret; if $z \geq 1$ the information rate is even higher. We also point out that the above scheme becomes *verifiable* after the following additional procedure, inspired by [9]. The dealer selects an appropriate elliptic curve E over the field $\mathbb{F}$ in such a way that the discrete logarithm problem for E is hard (see for instance [10], § 5.2), chooses a point Q on E and broadcasts Q and $Q_i := a_i Q$, $0 \leq i \leq k-1$. Any node receiving the share $p^{(h)}(u)$ can verify its integrity by simply checking

$$p^{(h)}(u)\, Q = \sum_{i=0}^{k-1} h! \binom{i}{h} u^{i-h} Q_i.$$

Fix now $V := \{u_1, \ldots, u_m\} \subset U$. Up to reordering we may assume that $u_i \in U_{l(i)}$ with $l(i) \leq l(j)$ for every $i \leq j$. Consider the square $k \times k$ matrix M_V whose i-th row is given by

$$\frac{d^{k_{l(i)-1}}}{dx^{k_{l(i)-1}}} \left(1, x, x^2, \ldots, x^{(k-1)}\right)(u_i). \tag{2}$$

In order to reconstruct the secret S, the combiner has to solve the following linear system:

$$M_V \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} p^{k_{l(1)-1}}(u_1) \\ \vdots \\ p^{k_{l(k)-1}}(u_k) \end{pmatrix} \tag{3}$$

This amounts to the Birkhoff interpolation problem with associated interpolation matrix $E_V = (e_{i,j})_{i=1}^{k} {}_{j=0}^{k-1}$ defined as follows:

$$e_{i,j} = \begin{cases} 1 & \textit{if } j = k_{l(i)-1} \\ 0 & \textit{otherwise} \end{cases}$$

It is easy to check by direct inspection that $V \in \Gamma$ if and only if E_V satisfies the Pólya condition. In particular, we deduce the following:

Theorem 1. *If $V \notin \Gamma$ then $\det(M_V)$ is identically 0, hence V cannot reconstruct the secret.*

Next we introduce some standard terminology. A *shift* Λ of E is a translation of a one from a place (i, j) into the place $(i, j+1)$, assuming that this is possible, i.e. $j + 1 < k$ and that $e_{i,j+1} = 0$; such operation produces a new matrix $\Lambda(E)$. We say that two rows of E have a *collision* if they have ones in the same column.

Define α to be the minimum number of shifts $\Lambda_1, \ldots, \Lambda_\alpha$ such that $\Lambda_\alpha \cdot \Lambda_{\alpha-1} \cdot \ldots \cdot \Lambda_1(E)$ has no collisions in rows 1 and 2. With this notation we have the following:

Lemma 1. *Let $M\boldsymbol{a} = \boldsymbol{b}$ be a Birkhoff interpolation problem with associated interpolation matrix $E = (e_{i,j})_{i=1}^{k} {}_{j=0}^{k-1}$ defined over a field $\mathbb{F}$ of characteristic $p = 0$ or $p > \max\{k-1, \alpha!\}$. Then $\det(M)$ is not identically 0 if and only if E satisfies the Pólya condition.*

Proof: The case of characteristic 0 is Theorem 10.1 in [11]. In the other case, following verbatim the same proof we obtain (see equation (10.4)):

$$\frac{d^\alpha}{dx_1^\alpha} \det(M) = \varepsilon C D$$

where $\varepsilon = \pm 1$, D is not identically 0 and C is the number of different representations of $\Lambda_\alpha \cdot \Lambda_{\alpha-1} \cdot \ldots \cdot \Lambda_1(E)$ as a composition of shifts. Our assumption on the characteristic of $\mathbb{F}$ implies that $\varepsilon C D$ (hence $\det(M)$) is not identically 0 for every $C \leq \alpha!$. In order to prove that this last inequality always holds, we may argue by induction

on α. If $\alpha = 1$, the result is trivial. For $\alpha \geq 2$, fix any composition Π of α shifts. We claim that in order to determine a representation $\Pi = \Lambda_\alpha \cdot \Lambda_{\alpha-1} \cdot \ldots \cdot \Lambda_1$ we have at most α choices for Λ_1. If it is true, then for every choice by induction we have at most $(\alpha-1)!$ choices to complete $\Lambda_\alpha \cdot \Lambda_{\alpha-1} \cdot \ldots \cdot \Lambda_1$, hence we obtain at most $\alpha!$ representations. Assume by contradition to have at least $\alpha+1$ choices for Λ_1, say $e_{s_i,t_i} \to e_{s_i,t_i+1}$, $i = 1, \ldots, \alpha+1$. Let $N_i(G) := \#\{g_{s_i,j} = 1 : j \leq t_i\}$ for every $d \times d$ square matrix G with entries $g_{i,j} \in \mathbb{F}$ and let $F := \Lambda_\alpha \cdot \Lambda_{\alpha-1} \cdot \ldots \cdot \Lambda_1(E)$. Then $N_i(F) < N_i(E)$ for every $i = 1, \ldots, \alpha+1$ and $\Lambda_\alpha \cdot \Lambda_{\alpha-1} \cdot \ldots \cdot \Lambda_1$ would be composed by $\alpha+1$ shifts, contradiction. □

In order to apply the above general results in our context, first of all notice that E_V satisfies Pólya condition if and only if $V \in \Gamma$ (essentially by definition). As a consequence, we can prove that a subset of participants can reconstruct the secret if and only if it belongs to the access structure. In particular, for $z = 0$ our scheme is *perfect*.

Theorem 2. *In the notation above, if $V \in \Gamma$ then $\det(M_V)(u_1, \ldots, u_k) \neq 0$, hence V can reconstruct the secret.*

Proof: If $t = 0$, then our scheme reduces to Shamir's one ([7]) and there is nothing to prove. If instead $t \geq 1$, up to reordering the rows of M_V we can assume that there are no collisions in rows 1 and 2, hence we have $\alpha = 0$. By Lemma 1, $\det(M_V)$ does not vanish identically and by [12], Proposition 1.2, it is a homogeneous polynomial of total degree $\frac{k(k-3)}{2}$. Since $u_1, \ldots, u_k$ are random, the conclusion follows from the next easy result. □

Lemma 2. *Let $p(x_1, \ldots, x_k)$ be a not identically 0 homogeneous polynomial of degree δ defined over a finite field $\mathbb{F}_q$ with $q > \delta + k$. Then there exists $(u_1, \ldots, u_k) \in (\mathbb{F}_q)^k \setminus \cup_{i,j}\Delta_{i,j}$ such that $p(u_1, \ldots, u_k) \neq 0$, where $\Delta_{i,j} := \{(x_1, \ldots, x_k) \in (\mathbb{F}_q)^k : x_i = x_j\}$*

Proof: By induction on d, the case $d = 0$ being obvious. Write

$$p(x_1, \ldots, x_k, y) = p_\delta(x_1, \ldots, x_k)y^\delta + \ldots + p_0(x_1, \ldots, x_k)$$

and for a fixed $(\bar{x}_1, \ldots, \bar{x}_k) \in (\mathbb{F}_q)^k \setminus \cup_{i,j}\Delta_{i,j}$ define $f(y) := p(\bar{x}_1, \ldots, \bar{x}_k, y)$. If $f(y) = 0$ for every $y \in \mathbb{F}_q \setminus \{\bar{x}_1, \ldots, \bar{x}_k\}$ then f has $q-k \geq \delta+1$ zeros and f vanishes identically. In particular, we have $p_i(\bar{x}_1, \ldots, \bar{x}_k) = 0$ for every i and if this is true for every choice of $(\bar{x}_1, \ldots, \bar{x}_k)$ in $(\mathbb{F}_q)^k \setminus \cup_{i,j}\Delta_{i,j}$ then by inductive assumption each $p_i(x_1, \ldots, x_k)$ is identically 0, contradiction. □

III. Hierarchical secret sharing in ad hoc networks

In an ad hoc network end-to-end security is a major issue. Indeed, we can assume that neighboring nodes can easily exchange security keys, in order to establish an authenticated and secure channel on a link basis (a usual assumption in this situation, see for instance [14] and [6]). Therefore, the problem to solve is related to grant secure transmissions on an end-to-end basis. Our approach aims at exploiting multiple independent paths from source to destination in such a way to spread along the ad hoc network the secret information. Depending on various factors, paths can be classified into several levels and identifying a suitable hierarchy of disjoint routes allows to apply the hierarchical secret sharing scheme presented in Section II in order to enforce security. However, the selection of a path hierarchy is a non trivial task in an ad hoc network. In the next paragraphs a general model is proposed, which is based on both global and local properties of the paths.

Let us identify a path from a source (dealer) A to a destination (combiner) B as an ordered sequence of nodes $\mathbf{x} = (x_1, \ldots, x_s)$, where $x_1 = A$ and $x_s = B$; two paths $(x_1, \ldots, x_s)$ and $(y_1, \ldots, y_t)$ are *independent* or *node disjoint* if $\{x_1, \ldots, x_s\} \cap \{y_1, \ldots, y_t\} = \{A, B\}$. As it is well known, the problem of finding a maximum cardinality

set of node disjoint paths in a network (thought as a digraph) can be solved in polynomial time (see for instance [13], Proposition 2.4 (i)). Choose a maximum cardinality set U of independent paths (or more generally any sufficiently big subset) and fix $n := \#U$.

We can assume that neighboring nodes can easily exchange security keys, in order to establish an authenticated and secure channel on a link basis (a usual assumption in this situation, see for instance [14] and [6]). Therefore, the problem to solve is related to grant secure transmissions on an end-to-end basis.

Let $p_{\text{loss}}(\mathbf{x})$ be the packet loss probability of the path $\mathbf{x}$. Its value depends on several properties of the path (for instance, signal-to-noise ratio, number of hops, interference, etc.).

It is possible to define $p_{\text{sniff}}(\mathbf{x})$ as the probability for a packet travelling on $\mathbf{x}$ to be eavesdropped. As a function of $\mathbf{x}$, p_{sniff} can be expressed as the algebraic sum of several contributions of different nature:

$$p_{\text{sniff}}(\mathbf{x}) = \sum_j F_j(\mathbf{x}) - \sum_{i,j} G_j(x_i)$$

normalized in such a way that $0 \leq p_{\text{sniff}}(\mathbf{x}) \leq 1$. The term F_j includes the potential flaws related to the whole path, such as the total number of hops, while G_j takes into account security robustness of each node, such as terminal's reliability, tamper resistant harware equippment, user's trustworthiness. It is clear that the functionals F_j contribute to p_{sniff} with positive sign (in particular, if the number of hops is higher, then a path is more likely to be subject to external attacks), while the functionals G_j are considered with the opposite sign.

The set of values assumed by p_{sniff} induces a natural hierarchy on the set of paths. Namely, if $p_{\text{sniff}}(U) = \{p_0, \ldots, p_t\}$ with $0 \leq p_0 < \ldots < p_t \leq 1$, then we can define:

$$U_l := \{\mathbf{x} \in U : p_{\text{sniff}}(\mathbf{x}) = p_l\}.$$

Finally, we have to determine a strictly increasing sequence of thresholds k_i. It is clear that higher thresholds produce a safer scheme; on the other hand, by definition, in order to recover the secret, the receiver needs at least k_i shares from $\cup_{l=0}^{i} U_l$. Hence, it seems reasonable to fix k_i as the expected number of shares reaching the destination via paths of level i or less. More precisely, we define:

$$k_i := \lfloor \sum_{\substack{x \in U_l \\ 0 \leq l \leq i}} (1 - p_{\text{loss}}(\mathbf{x})) \rfloor, \tag{4}$$

where $\lfloor r \rfloor$ denotes the biggest integer $\leq r$.

Summarizing, the proposed scheme can be implemented as follows:

Source A:

1) finds a set U of node disjoint paths to destination B with a multipath routing process (see for instance [15] and [16]) and for each $\mathbf{x} \in U$ collects all relevant properties of $\mathbf{x}$ (signal-to-noise ratio, number of hops, interference, terminal's reliability, user's trustworthiness...);
2) computes $p_{\text{loss}}(\mathbf{x})$ and $p_{\text{sniff}}(\mathbf{x})$ for every path $\mathbf{x} \in U$;
3) defines $(k_0, \ldots, k_t; n)$ with k_i as in (4) and $n := \#U$;
4) selects a finite field $\mathbb{F}$ with characteristic $p \geq k_t$ and cardinality $q \geq \frac{k_t(k_t-1)}{2}$ and identifies the secret with an element $S \in \mathbb{F}$;
5) picks a polynomial

$$p(x) = \sum_{i=0}^{k-1} a_i x^i$$

where $k = k_t$, $a_0 = S$ and a_i arbitrary elements of $\mathbb{F}$ for $1 \leq i \leq k-1$;

6) identifies each path $\mathbf{x} \in U_l$ with a random element $u \in \mathbb{F}$ and associates to u the share $p^{(k_{l-1})}(u)$, where $p^{(h)}$ denotes the h-th derivative of p and $k_{-1} := 0$;
7) transmits every share along an independent path through source routing, exploiting private communication between neighbouring nodes (as in [14], [6], it is possible to assume that neighbouring nodes in an ad hoc network can exchange encryption keys during link initialization in order to establish an authenticated channel on the physical link).

Destination B:

1) receives $m \leq n$ shares, say from the subset of paths $V := \{u_1, \ldots, u_m\} \subseteq U$;
2) constructs the matrix M_V as in (2);
3) recovers the secret by solving the linear system (3) in the indeterminates $a_0, \ldots, a_{k-1}$.

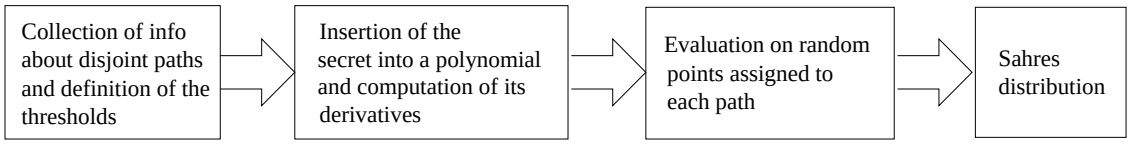

Fig. 1. Flow diagram of Source A

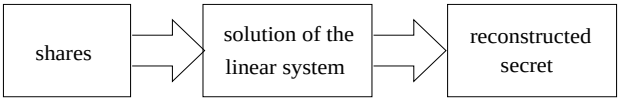

Fig. 2. Flow diagram of Destination B

Notice that any intruder eavesdropping up to $k_i - 1$ shares from $\cup_{0 \leq l \leq i} U_i$ has no information about the confidential message sent over the network (according to Theorem 1).

IV. A Possible Application Scenario

This section provides a possible application scenario for the proposed hierarchical secret sharing scheme.

Let us assume to have an ad hoc network of N nodes uniformly distributed in a planar region of area R, for example sensors disseminated in a terrain which need to communicate protecting data. In this situation, the problem of finding independent paths between a pair of nodes has been addressed in several papers. In [6] a modified Dijkstra algorithm is used; however, this solution assumes the knowledge of the graph associated with the network, which is not always available in such a network. Different approaches are proposed, like [15] (Selective Broadcast) and [16] (AODVM), just to quote some recent contributions. In particular, simulation results are available for $N = 50$ and $R = 1500 \times 500\ m^2$ ([15], § VI) and for $N = 250, 350, 500$ and $R = 2500^2\ m^2$ ([16], § IV).

Here instead we are going to determine a suitable choice of parameters for the implementation of our scheme in this context, providing also a numerical example (see Table I). We denote by $\rho = N/R$ the node spatial density and by r the average distance between any pair of neighbouring nodes. As motivated in [17], II.A, the relationship between ρ and r is approximately $r \approx \frac{1}{\sqrt{\rho}}$. As a consequence, an estimate for number h_0 of hops in the shortest path between two nodes A and B having mutual distance d is given by $\lceil \sqrt{\rho}\, d \rceil$, where $\lceil s \rceil$ denotes the smallest

integer $\geq s$. An arbitrary path $\mathbf{x}$ between A and B is a sequence of $h(x) \geq h_0$ hops, and it is possible to split the set U of independent paths between A and B into levels as follows:

$$V_i := \{\mathbf{x} : h(\mathbf{x}) = h_0 + i\}.$$

Moreover, if p is the probability for each node to be active, it is natural to set the packet loss probability increasing with the number of hops:

$$p_{\text{loss}}(\mathbf{x}) = \left(1 - p^{h(x)}\right).$$

In order to implement the proposed scheme, we introduce the integer:

$$i_0 := \min\left\{ i : \sum_{\substack{x \in V_l \\ 0 \leq l \leq i}} (1 - p_{\text{loss}}(\mathbf{x})) \geq 1 \right\} \tag{5}$$

and we define a hierarchical structure based on length of paths:

$$\begin{aligned} U_0 &:= \cup_{0 \leq i \leq i_0} V_i \\ U_1 &:= \cup_{i > i_0} V_i. \end{aligned}$$

Hence the set U naturally splits according to two priority levels into U_0, corresponding to paths with lower number of hops and therefore lower probability of eavesdropping, intrusion and capturing, and U_1, collecting all remaining ones. The discriminant number of hops is chosen as the minimum value compatible with the condition that the threshold k_0 defined in (4) is a positive integer. In this simplified scenario, we have $p_{\text{sniff}}(U_0) = \{p_0\}$ and $p_{\text{sniff}}(U_1) = \{p_1\}$ with $0 \leq p_0 \leq p_1 \leq 1$, but the proposed scheme gives the freedom to establish the path hierarchy according to different parameters (for instance, high priority could be granted to paths with high performance: high signal-to-noise ratio, low delay,...), as well as a combination of the above.

In Figure 3 we report a set of 70 nodes uniformly distributed in a 1000×1000 meters terrain. We find 5 independent paths between the fixed source A and destination B. The number of hops in the shortest path x_3 is equal to 5, exactly as estimated above, and 3 sets of paths V_0, V_3, V_5 are defined. Now it is possible to compute p_{loss} for each path and calculate i_0 by applying (5). The path hierarchy is now completely determined (see Table I). In order to quantify the security enforcement produced by our hierarchical approach, we compare the probabilities of reconstructing the secret after capturing r nodes in three different cases: Shamir's standard scheme (where just 3 nodes are needed among $x_1, \ldots, x_5$), Shamir's hierarchical scheme (where 2 shares are assigned to paths x_2, x_3, x_4 and just one to paths x_1, x_5, so at least 4 shares, being expected to reach the destination, are requested to recover the secret) and our hierarchical scheme (where at least 2 nodes are needed among x_2, x_3, x_4 and at least 3 among $x_1, \ldots, x_5$). We make the assumption that source A and destination B cannot be captured. The remaining $n = 68$ nodes, having the same probability of being captured, naturally split into 6 subsets, 5 corresponding to the independent paths $x_i, i = 1, \ldots, 5$ (respectively with cardinalities $n_1 = 9, n_2 = 7, n_3 = 4, n_4 = 7, n_5 = 9$) and the last are x_6 collecting external nodes (with cardinality $n_6 = n - n_1 - n_2 - n_3 - n_4 - n_5 = 32$). In this model, the probability of getting r_i nodes from the set x_i ($i = 1, \ldots, 6$) by capturing exactly $r = r_1 + r_2 + r_3 + r_4 + r_5 + r_6$ nodes is given by the formula

$$P = \frac{\prod_{i=1}^{6} \binom{n_i}{r_i}}{\binom{n}{r}}$$

Hence, by adding the contributions of all relevant cases, we obtain the probability of reconstructing the secret as a function of r as reported in Figure 4. It is apparent that Shamir's hierarchical scheme is unsuitable for this application, while our approach outperforms the standard non-hierarchical scheme. For instance, after capturing 10% of nodes, the probability of secret reconstruction is 32% for our method against 49% for Shamir's one.

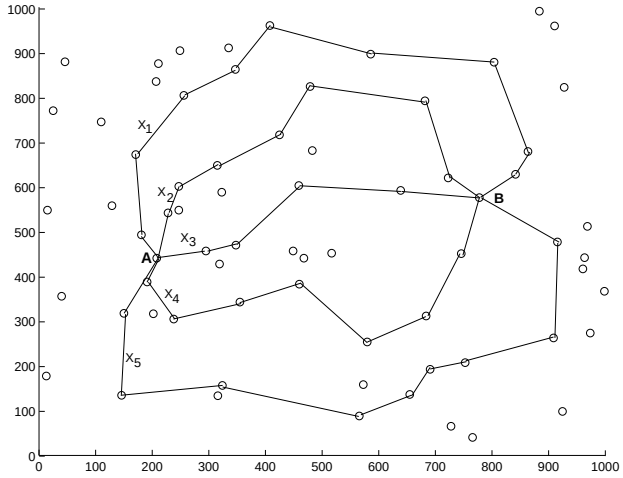

Fig. 3. Example of uniform distribution

TABLE I

VALUES CORRESPONDING TO FIGURE 3

$R = 1000^2\ m^2$
$N = 70$
$\rho = 7 \times 10^{-5}$
$r \approx 119,5\ m$
$h_0 = 5$
$V_0 = \{x_3\}$, $V_3 = \{x_2, x_4\}$, $V_5 = \{x_1, x_5\}$
$p = 0,95$
$p_{\text{loss}}(x_3) \approx 0,23$
$p_{\text{loss}}(x_2) = p_{\text{loss}}(x_4) \approx 0,34$
$p_{\text{loss}}(x_1) = p_{\text{loss}}(x_5) \approx 0,4$
$i_0 = 3$
$U_0 = V_0 \cup V_3$, $U_1 = V_5$
$k_0 = 2$, $k_1 = 3$

V. CONCLUSIONS AND FUTURE WORK

The paper presents an innovative approach that exploits multi-path routes in order to defi ne a flexible framework for end-to-end secure transmission in ad hoc networks by distributing the shares in a hierarchical way. This is achieved by designing an ideal, perfect, and eventually verifi able secret sharing scheme based on Birkhoff polynomial interpolation and by establishing suitable hierarchies among independent paths. An explicit algorithm is provided and a numerical example is presented in order to validate it.

Future work on the topic will deal with the implementation of the proposed scheme in a simulation environment.

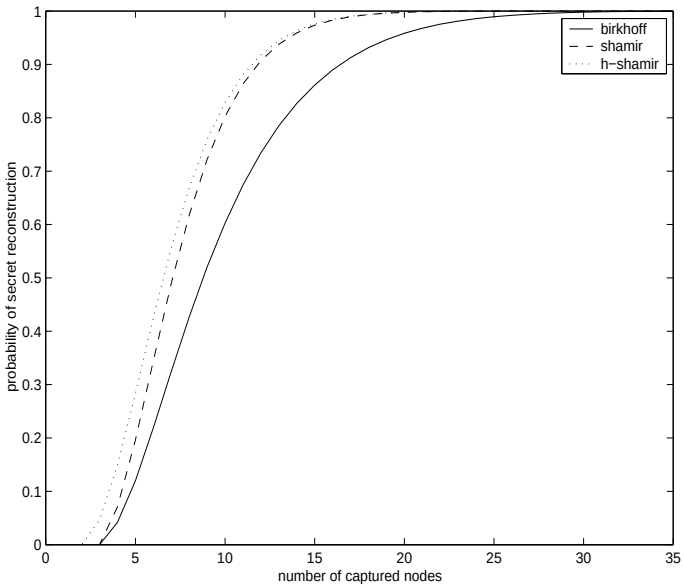

Fig. 4. Probability of reconstructing the secret after capturing $r = 0, \ldots, 34$ nodes in Shamir's standard scheme (shamir), Shamir's hierarchical scheme (h-shamir) and our hierarchical scheme (birkhoff)

REFERENCES

[1] RFC2401 *Security Architecture for the Internet Protocol*

[2] R. Molva and P. Michiardi. *Security in Ad Hoc Networks*. Invited Paper in Personal Wireless Communication (PWC'03), September 2003, Venice, Italy.

[3] S. Yi, P. Naldurg, and R. Kravets. *Security-Aware Ad-Hoc Routing for Wireless Networks. Technical Report of the University of Illinois at Urbana-Champaign, 2001.*

[4] L. Buttyan and J.-P. Hubaux. Report on a Working Sesson on Security in Wireless Ad Hoc Networks. *Mobile Computing and Communications Review, Vol. 6, No. 4, 2002.*

[5] L. Zhou and Z. Haas. Securing Ad Hoc Networks. *IEEE Network 13(6) (1999), 24–30.*

[6] W. Lou and Y. Fang. Securing Data Delivery in Ad Hoc Networks. *Proc. of the Ninth International Conference on Distributed Multimedia Systems, September 2003, Miami (USA), 599–604.*

[7] A. Shamir. How to share a secret. *Communications of the ACM 22 (1979), 612–613.*

[8] T. Tassa. Hierarchical Threshold Secret Sharing. *Proc. of the Theory of Cryptography Conference 2004, MIT, Cambridge MA, USA, February 2004, LNSC 2951, Springer-Verlag, 2004, 473–490.*

[9] T. P. Pedersen. Distributed Provers with Application to Undeniable Signatures. *Proc. of Eurocrypt '91, Lecture Notes In Computer Science, LNCS 547, Berlin: Springer-Verlag, 1991, 221–238.*

[10] N. Koblitz, A. Menezes, and S. Vanstone. The State of Elliptic Curve Cryptography. *Designs, Codes and Cryptography 19 (2000), 173-193.*

[11] R. A. DeVore and G. G. Lorentz. Constructive Approximation. *Grundlehren der Mathematischen Wissenschaften 303, Springer-Verlag, Berlin, 1993.*

[12] G. G. Lorentz, K. Jetter, and S. D. Riemenschneider. Birkhoff interpolation. *Encyclopedia of Mathematics and its Applications 19, Addison-Wesley Publishing Co., Reading, Mass., 1983.*

[13] J. Cheriyan. Randomized algorithms for problem in matching theory. *SIAM J. Comput. Vol. 26, No. 6, December 1997, 1635-1655.*

[14] M. Hietalahti. Key Establishment in Ad Hoc Networks. *Technical Report, Helsinki Univ. of Technology, Dept. of Computer Science and Engineering, 2001.*

[15] K. Wu and J. Harms. Multipath Routing for Mobile Ad Hoc Networks. *IEEE ComSoc/KICS Journal of Communications and Networks, Special Issue on Innovations in Ad Hoc Mobile Pervasive Networks, Vol. 4, No. 1, March 2002, 48-58.*

[16] Z. Ye, S. V. Krishanamurthy, and S. K. Tripathi. A Framework for Reliable Routing in Mobile Ad Hoc Networks. *IEEE INFOCOM 2003.*

[17] G. Ferrari and O. K. Tonguz. Minimum Number of Neighbors for Fully Connected Uniform Ad Hoc Wireless Networks. *Proc. IEEE Intern. Conf. Commun. (ICC'04), Paris, France, June 2004, 4331–4335.*