Reed-Solomon Codes and Multi-Path Strategies to Improve Privacy Performance over Ad Hoc Networks

Hervé Aïache, Cédric Tavernier and Corinne Sieux
System Engineering and Architecture Dept.
THALES Communications S.A.
Colombes, France
{herve.aiache, cedric.tavernier, corinne.sieux}@fr.thalesgroup.com

Abstract— **This paper presents a privacy protection scheme, suitable for devices limited in CPU and/or in memory capabilities, which not only ensures anonymity and confidentiality but has also a limited impact on end-to-end network performance. Such an approach for anonymous communications, inspired by network coding techniques, benefits from recent improvements in list decoding algorithms for Reed-Solomon codes, and takes advantage of multi-path routing capabilities. The combination of these techniques is adapted for constrained and pervasive environments, such as wireless ad hoc networks, as it decreases the processing complexity of the cryptographic/decoding operations and as it ensures better tolerance to packet losses (due to mobility or to bad quality of the radio channel).**

Keywords— **Privacy, Anonymity, Confidentiality, Ad hoc networks, Reed-Solomon codes, Multi-path routing.**

I. INTRODUCTION

Nowadays, privacy and security solutions require to protect personal information so that may not be disclosed to unauthorized part, which could passively collect them for undesired and illegal purposes. It is a challenge to address these issues in networks with strong constraints like wireless ad hoc networks. In fact, this kind of network environment introduces more difficulties/constraints due to the intrinsic nature of this kind of environment, which is de facto more vulnerable than its wired homologue. First, this is especially true concerning passive attacks due to the fact that an attacker is able to capture easily and remotely wireless transmissions without disturbing the wireless ad hoc network, in other words without being detectable. Second, designing cryptographic functions or mechanisms for the context of wireless ad hoc networks is very challenging due to performances constraints, which are, on one hand, required for high data rate exchanges but, on the other hand, impacted and reduced by the common use of small mobile devices embedding low CPU and/or memory capabilities to compose the ad hoc infrastructure. Most of the existing solutions proposed for ad hoc wireless networks are based on on-demand scheme, relying on reactive routing protocol approach [1][2][3][4][5]. Their anonymity schemes are mainly originated from Mix-net approach [6][7][8], which needs to be improved in term of performance to be suitable in the context of constrained and pervasive network environments, such as wireless ad hoc networks.

This paper proposes and defines a complete method that provides privacy/security, which has a limited impact on performances. This approach for anonymous communications, inspired by network coding techniques, benefits from recent improvements in list decoding algorithms for Reed-Solomon codes, takes advantage of multi-path routing capabilities. The solution aims to ensure privacy/security of information that has interest only during a relatively short time. The main objective of the approach is to discourage attackers by requiring too many efforts to recover the information compared to the time when the information is useful. Moreover, note that this solution assumes the availability of a multi-path routing or forwarding protocol. Multiple paths between a source, destination couple ensure packet diversity, in order to improve anonymity: the task of eavesdroppers is therefore hardened by hiding them the information of which packet belongs to which flow.

In view to present this approach, the section II explains and reminds the cornerstones of the solution. Then, the section III of this paper provides an overview of the anonymous communications scheme. The section IV describes an information splitting strategy, which aims at reinforcing privacy protection. The section V details a method to reduce the calculation processing required by the cryptosystems to ensure source anonymity and source/destination unlinkability. The section VI evaluate under simulation environment the impact of the splitting strategy over a multi-path routing on the global end-to-end network performance. The conclusion of this paper summarizes the main results and explained the future works.

II. PRIVACY PROTECTION AND REED-SOLOMON CODES

A. Multi-path strategies and Privacy issues

A recent and popular idea consists in encoding information of length k bytes by a polynomial of degree $k-1$ over a finite field F_q and in using a Lagrange interpolation to reconstruct the sent information [9]. Such an interesting approach is equivalent to encode information with a Reed-Solomon code $RS_q[k,k]$ of length k and dimension k. In the wired context, this approach appears powerful since an attacker has to corrupt many nodes in order to reconstruct the information.

Unfortunately, in wireless context, eavesdropping technique is less expansive and an attacker is able easily to intercept and to identify the transmissions between nodes. This is why, in wireless environment encoding by a Reed-Solomon code and splitting the information is not sufficient to disturb an attacker.

978-1-4244-1653-0/08/$25.00 ©2008 IEEE

Nevertheless, in main cases, a security proof can be obtained if we assume that the attacker has only access to a small fraction of the transmission, such as in [10] for sensor networks. In view to counter this main issue, the SPREAD protocol [9] aims to build a maximum of disjoint routes. Unfortunately, finding these disjoint paths is a very strong constraint in many cases. But, on the other hand, multi-path forwarding strategies can ensure improvements of the global performance. In view to reinforce the combination of these techniques, this paper details the elaboration of an anonymous communication scheme relying on the difficulty to decode the Reed-Solomon code. Therefore, the following section explains the properties of the Reed-Solomon codes.

B. *Properties of the Reed-Solomon codes*

In fact, the Reed-Solomon codes appears interesting to ensure privacy protection over constrained and pervasive environments, such as ad hoc networks. Before entering into the details the anonymous communications scheme we propose in this paper, we first reminds the definition of Reed-Solomon codes and then formal core results around their properties.

Reed-Solomon codes are defined as follows: Let F_q be the finite field of q elements. Let $x_1, \ldots, x_n$ be n distinct elements of F_q. We denote by $ev : F_q[X] \rightarrow F$, the evaluation function

$$ev : p(X) \rightarrow (p(x_1), \ldots , p(x_n)),$$

where F_q is the ring of the univariate polynomials over F_q. We denote $RS_q(k,n)$ the Reed-Solomon code of dimension k and length n over F_q. By definition

$$RS_q(k,n) = \{ev(f); f \in F_q[X]; deg f < k\}.$$

The minimal distance of this code is given by $n-k+1$, then we are guaranteed to have a single decoding if we decode up to $n-k+1$ errors. And the formulation of the Reed-Solomon Decoding problem (RSD) is the following: Given a $RS_q(k,n)$ code, ω an integer and a word $y \in F^n_q$, find any codeword in $RS_q(k,n)$ at distance less than ω of y.

Based on the complexity theory, it is important to remind a main result related to the Polynomial Reconstruction problem (PR) that we can find in [11]. The Polynomial Reconstruction problem (PR) is defined as follows: Given n, k, t and (x_i, y_i), $i=1,\ldots,n$ with distinct x_i's, output any polynomial $p(X)$ such that $deg(p) < k$ and $p(x_i) = y_i$ for at least t values of the index i. Thus we have that $PR = RSD$. It is known that PR is polynomial in n, k if $t > \sqrt{kn}$ (see [13]). It is also polynomial if $t = \sqrt{kn}$ with a complexity in $O(n^{15})$ [13]. To understand the difficulties to solve the general problem of PR, let describe the Poly Agree problem (PA).

The Poly Agree problem (PA) is defined as follows: Given n, k, t and a set of pairs $P = \{(x_1, y_1),\ldots, (x_n, y_n)\}$, $x_i, y_i \in F_q$, does there exist a degree k polynomial $p(X)$ such that $p(x_i) = y_i$ for at least t different i's? It is important to note that for this problem, the x_i's are not required to be different, so this problem is not equivalent to PR. In [12], PA is proved to be NP-hard so this result seems to indicate that PR is a hard problem. The rest of this paper focuses on the elaboration of an anonymous communications scheme (its related protocols and methods) based on the difficulty to reconstruct a polynomial (PR).

III. COMBINING PERFORMANCE AND PRIVACY PROTECTION

Our idea here is inspired by the SPREAD protocol [9]. The main differences come from the resistance against the noise due to the channel, a more realistic hypothesis concerning the fraction of data that an attacker could intercept. We also reinforce the security issues since the problem of the attacker is considered now to be very hard.

A. *Reed-Solomon encoding*

We propose to encode the information with a Reed-Solomon code $RS_q(n,k)$ defined over F_q where q is usually equal to 28, of length $n < q$, dimension k and minimal distance $n-k+1$. The generator matrix of this code will be chosen non-systematic in order to make the encoded message not directly readable. We can correct with this code $n-\sqrt{kn}$ errors with a complexity of order $O(n^2 log^2(n))$ byte operations [13].

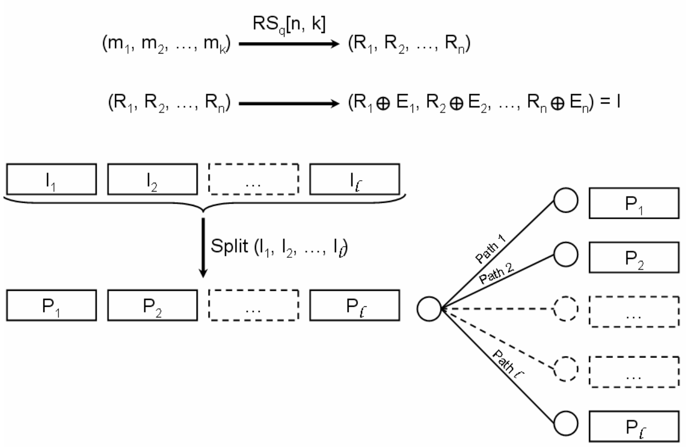

Figure 1. Information splitting technique.

Now let's assume that in average there is $n\delta$ byte errors on a information of size n and that we want to transmit an information through l paths. Then we propose to add a random error $E=(E_1,\ldots,E_n)$ of Hamming weight $W = n-\sqrt{kn}-n\delta$ while $W \geq 0$. In our principle, the packet that we have to send have a fixed size, by example proportional to n. Then each path can support $n\delta$ byte errors on each encoded message of length n. We call $Share$ the function which add random byte errors and rearrange the transmitted message. Whence, in considering a message m of length n bytes, we can summarize the steps of encoding in the following way: we first encode m with a Reed-Solomon $RS_q(n,k)$ code that gives a n length vector $R=(R_1,\ldots,R_n)$, then we add byte by byte to this vector the random error E. We get the vector $I = (I_1,\ldots,I_n)$ which will be split in l shares $(I_1,\ldots,I_l)$. These steps are graphically summarized in Figure 1. Of course this is a simplified description, since many control messages should be added in order to insure the coherence, in order to synchronize in simple way the data and so on.

B. Privacy and network performance trade-off

For network performance, there is obviously a gain, since the coding algorithm supports intrinsically errors on transmission. Moreover, since it is possible to monitor the radio channel in term of errors, we are able to improve the bandwidth requirement. This is particularly true if the end-device (e.g. laptop or PDA) are equipped with several antennas. However, in case of equipments integrating a single antenna, a discussion is needed and we will give some simulation results in section VI.

On the other hand, privacy protection is now hardened. In fact, if an attacker envisages to reconstruct the complete information, the interception, in average, of the totality of the messages is mandatory. This is mainly due to the fact that each codeword P_j, $j \in [1,\dots,l]$ of the Figure 1 contains a fraction of a complete noisy codeword I. Moreover, based on the interception of messages fractions, an attacker cannot reconstruct the message in polynomial time since, as shown in the previous section, this reconstruction problem is very difficult. In this way, note that a number of *errors+erasures* greater than the threshold $n-\sqrt{kn}$ corresponds to the limit for which the decoding algorithm works in polynomial time.

IV. INFORMATION SPLITTING STRATEGY DESCRIPTION

First, a plain message is divided into fragments of length k, corresponding to the dimension of the chosen Reed-Solomon code $RS_q(n,k)$. Then each fragment is encoded with $RS_q(n,k)$ as an information piece I_j of length n. If n is set to lp (i.e. $n = lp$), we can share each encoded fragment I_j in l parts of length p:

$$I_j = [I_j^{(1)}][I_j^{(2)}][\dots][I_j^{(l)}].$$

and the information blocks P_j, $j \in [1,\dots, l]$ will be given by

$$P_j = [P_1^{(j)}][P_2^{(j)}][\dots][P_l^{(j)}].$$

Note that for implementation issues, a control message should be added to each information block P_j.

Thanks to such a splitting strategy, if an attacker intercepts some parts of the encoded information, the amount of fragment will be not exploitable in average as explained before. In this way, the attacker will not be able to reconstruct the original data, keeping private the information sent. Moreover, this information fragment is unreadable for two main reason: the generator matrix of the Reed-Solomon code was chosen non-systematic and we can chose $p < k$ even for non-noisy information block of k bytes of P_j. Unfortunately, such a splitting strategy is not sufficient in the context of wireless networks since eavesdropping is not so difficult to implement. In fact, over such a medium, an attacker, by potentially intercepting all transmissions, could decode the plain message as well as the receiver. This means that the information and the control message need to be encrypted by a fast public key cryptosystem, as described in the following section.

V. FAST PUBLIC KEY CRYPTOSYSTEM OPERATIONS

As mentioned previously, the main idea is to encrypt the control messages and the nodes' addresses with a public key cryptosystem. Let note it $Y = F(K_{pub},X)$, where K_{pub} is the public key, X the plain message and Y the encrypted message. The inverse of F is $F^{-1}(K_{priv},X)$, where K_{priv} is the private key, and satisfies $F^{-1}(K_{priv},F(K_{pub},X)) = X$. Due to the fact that most of the usual and well known public key cryptosystems are relatively slow, we suggest to use in this method a less known but strong and fast public key cryptosystem proposed by McEliece in 1978 [14]. Such a cryptosystem is interesting since it is able to encrypt information more faster than RSA, Elliptic Curves and ElGamal cryptosystems. In addition to this basis, we assume that each node owns its private key, and that all nodes know the complete set of public keys.

A. Reinforcing the anonymous communications scheme

Let assume that the source A wants to send a message m to the node B through the path ACB. Let N_j be a node's address for $j \in \{A,B,C\}$. Since we do not consider ad hoc networks composed by a large number of nodes, it is reasonable to concatenate each node address with a random string. In this way, in our example, A send to C the vector $(m, Y = F(K_{pub}(C), (NB|random)))$. C is a node able to decrypt this received vector, which gives $(m, F^{-1}(K_{priv}(C),Y)) = (m,(NB|random))$. Finally, C send m to B.

Through this method, each intermediary node always knows the final destination of a message. However, it cannot determine who really sent this information. In fact, each intermediary node is not able to identify if the previous node was the source or another intermediary node. In this way, the anonymity and the source/destination linkability cannot be broken (even if the node C falls under the control of an attacker). Moreover, in a complete scenario involving a more meshed network, and by applying the splitting strategy described in section IV, C will only access to a fraction of the messages, which is not sufficient to reconstruct the complete information.

B. Securing the control messages

For the control messages, we suggest to use a symmetric cryptosystem, noted $Ciph(K_s,X)$ (e.g. AES). The basic idea is to encrypt a secret key K_s with the public key of the destination, which will be sent by the source. With this method, the intermediary nodes cannot obtain the control messages. The encryption operation is described in the following.

We note m the message, C_m the control messages, K_s the secret key, N_d the address of the destination node, rd and rd' two random bit strings. Based on this notation, a source node will construct some frames of the form $(m|C_m|K_s|N_d)$, where the symbol $|$ indicates the concatenation.

In our example, the source A will send to the neighbour node C:

$$(m|Ciph(K_s,C_m)|F(K_{pub}(B),K_s|rd)|Ad(C)),$$

with $Ad(C) = F(K_{pub}(C),N_d|rd')$, where B is the destination and rd' is a random bit string. The destination node B will receive

$$(m|Ciph(K_s,C_m)|F(K_{pub}(B),K_s|rd))$$

And the node B will perform the following operations:

$$K_s = F^{-1}(K_{priv}(B), F(K_{pub}(B), K_s|rd))$$

and

$$C_m = Ciph^{-1}(K_s, Ciph(K_s, C_m))$$

in order to get (m, C_m).

This particular technique increases the difficulty for an attacker to reconstruct the initial information. In fact, the received frames have now to be re-ordered to retrieve some noisy codeword of the Reed-Solomon code. This constitutes a very difficult task due to the fact that the attacker does not know the control messages.

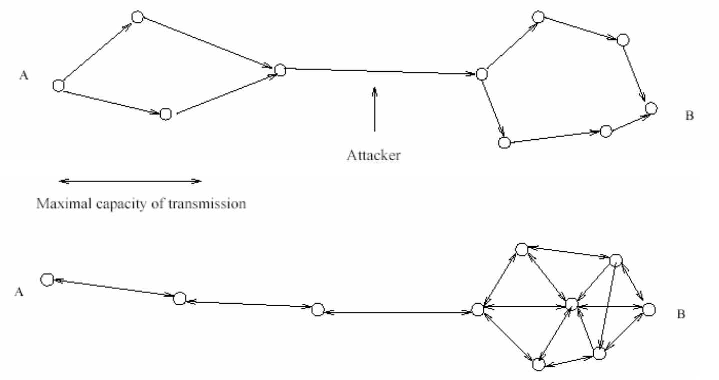

Figure 2. No disjoint paths exist between nodes A and B.

Note that this anonymous communications scheme assumes intrinsically that the length of the public and of the private key of F is greater than the length of the block, which can be encrypted by $Ciph$. In most cases, this assumption is correct (e.g. $F \equiv RSA$ and $Ciph \equiv AES$). However, it would be false for $F \equiv DCC$ [18] (with 160 bits for its public and private keys) and $Ciph \equiv Rijndael$ [19] (with the 256 bits for the blocks). For these particular contrary cases, we suggest to apply several times the encryption function of the public key cryptosystem and to concatenate random bit strings. These random bit strings are important for ensuring anonymity since they allow to attribute a sufficient number of keys to a specific nodes. Moreover, to complete the proposed method, an efficient key management scheme, such as [17], should be added.

At last, it is important to note that this anonymous communication method would fail if only two device communicate in the ad hoc network. In fact, in this case, a simple passive traffic analysis could break the anonymity: an attacker observing the ad hoc network could identify who communicates with whom. To solve this issue, we suggest to apply the well-known "dummy traffic" techniques [15][16] (i.e. injection of fake packets). Such techniques make harder the traffic analysis attacks and improve unobservability aspect.

However, if the ad hoc network topology is weakly dense, in the sense that multiple routes do not exist between each $(source, destination)$ couple, "dummy traffic" technique is not efficient. In fact, if no disjoint paths exist between a source and a destination node, as illustrated in the Figure 2, anonymity has no sense and we need to encrypt the exchanged messages, in view to keep information confidentiality. Therefore, to complete our anonymous communications method, we introduce a threshold cryptography concept: if there is not more than l disjoint paths, then we will cipher the information and the control messages with the symmetric cryptosystem (the secret key will be chosen by the sender and communicate in using the asymmetric cryptography).

Note that we keep the splitting strategy in the area where sufficient multiple routes exist between intermediary nodes in view to improve the global performance. We predict that in average most communications will not required a complete encryption, then the transmission process should stay relatively light.

VI. SPLITTING, MULTI-PATH STRATEGY AND SIMULATIONS

This section focuses on the evaluation of the proposed anonymous communication scheme over a multi-path routing algorithms. The main objective is to validate the trade-off between privacy protection and network performance. More specifically, this section will evaluate the impacts of the splitting strategy on the throughput.

A. *Splitting strategy and multi-path routing assumptions*

We assume that a proactive routing protocol is used by the ad hoc network (e.g. OLSR [21]). Such a routing protocol should has also multi-path capabilities (i.e. several routes can be discovered between a source and a destination). Moreover, we consider that it can diffuse performance metrics, evaluated on each radio links. The Figure 3 illustrates and summarizes all these considered properties.

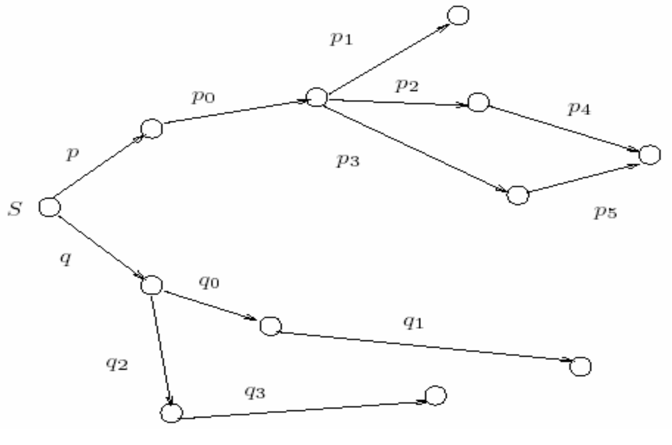

Figure 3. Multi-path routing protocol.

Providing a proof that splitting strategy implemented over a multi-path routing is more efficient than usual best path is not trivial, and especially in the case of devices integrating a single antenna. However, for example, if the noise is not uniformly distributed, then it is clear that a splitting strategy increases the possibility to send some re-constructible information. By construction, each value p_i or q_i depends on the quality of the next paths, then we can study this problem locally by considering the Figure 4.

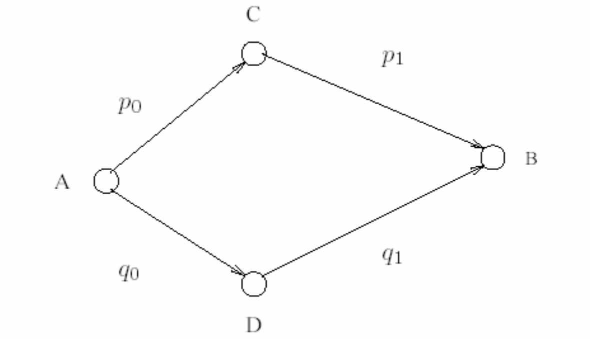

Figure 4. Splitting strategy model

Each edge is affected with a value corresponding to the flow on the link. Then the flow p of the path ACB is equal to $p = min(p_0,p_1)$ and similarly, the flow q of the path ADB is equal to $q = min(q_0,q_1)$. Let assume that the process which consists in sending alternatively packets to the nodes C and D is negligible compared to the time to send data from A to C or D. This is a reasonable hypothesis if we consider that the different edges can aggregate many connections (e.g. if the flow is relatively slow). Then the global flow of information is given by $p+q$ by counting the quantity of information at the nodes C and D. The unknown of this system is the global flow between A and B since the nodes C and D could face conflicts to access to the node B. In the following section, we propose to study this main issue through simulation environment based on IEEE 802.11 ad hoc networks.

B. Simulation environment and scenario

As mentioned previously, we are interesting to evaluate the performance of the splitting strategy over multi-path routing. For that purpose, we developed a particular simulation model focused on our splitting strategy for a mobile ad hoc network.

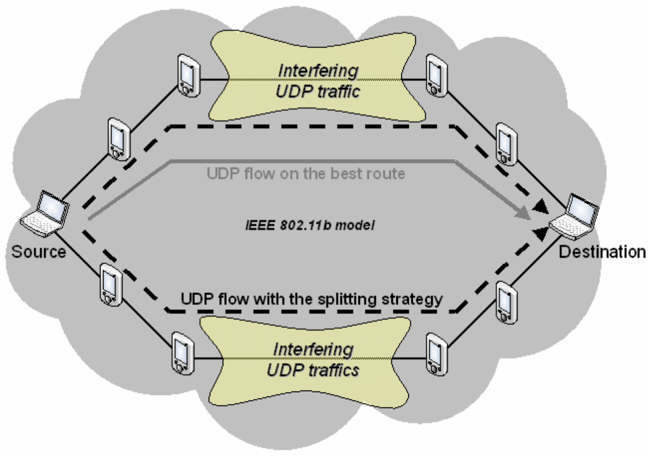

Figure 5. Simulation model and scenario.

This model was implemented over OMNET++ [20], an open-source discrete event simulation environment. The simulations rely on the INET framework libraries relative to IEEE 802.11b, which operates in the 2,4 GHz band.

The Figure 5 illustrates the scenario used for the simulations. In this scenario, a UDP traffic is initiated by the source node to the destination. Interfering UDP flows have been injected on different links composing the routes in view to

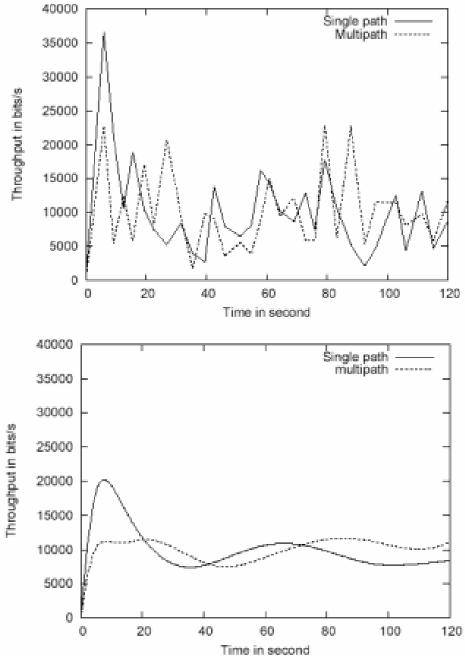

Figure 6. Throughput measured on run 1.

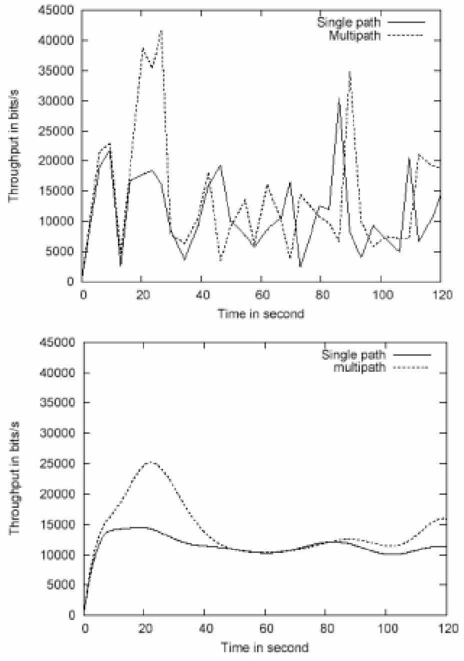

Figure 7. Throughput measured on run 2.

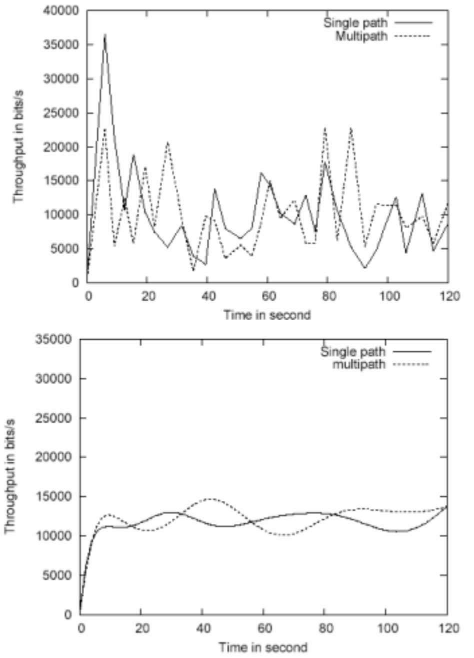

Figure 8. Throughput measured on run 3.

impact on their global quality. First, the UDP traffic between the source and the destination nodes followed the best route, identified as the less impacted one. Then, the UDP traffic was split with respect to our strategy over the two routes (i.e. sending alternatively some data on each path). The simulation measurements consisted in comparing the end-to-end throughput observed between the source and the destination nodes.

C. *Simulation results and analysis*

Figure 6, Figure 7 and Figure 8 summarize the results obtained through three runs of simulation. Since the curves obtained directly with OMNET++ do not provide an accurate view of the global throughput behaviour, we systematically add a Bezier approximation (shown on the bottom of each figure). For the Figure 6, the average flow with the splitting strategy over multi-path allows to obtain a gain of 8,54%: 11162 bits/s against 10284 bits/s with a single path. For the Figure 7, the average flow with the multi-path strategy provides a gain of 24,49%: 14181 bits/s against 11391 bit/s with a single path. For the Figure 8, we observe an average flow with the multi-path strategy that decreases the performance of 5,50%: 12270 bits/s against 12985 bits/s with a single path. Based on these simulation results we do not observe significant losses. In average, the obtained results shows good improvement on the end-to-end network performances.

VII. Conclusion

In this paper, we elaborated and proposed a new anonymous communications scheme, which targets an acceptable trade-off between privacy protection and end-to-end performance. Such an approach relies on the difficulties to reconstruct a noisy message, explicitly encoded with a Reed-Solomon code. Moreover, inspired by network coding techniques, the approach benefits of a particular splitting strategy implemented over multi-path routing in view to combine network performance to the implicit reduction of the calculation processing required to encode and to encrypt data. In this way, our solution appears to be suitable for devices limited in CPU and/or in memory capabilities and adapted to highly pervasive environments, such as ad hoc networks.

In addition, the proposed privacy protection scheme can be considered as a generalization of [9], which extend it, through a threshold cryptography concept, by considering more complex and constrained cases, usual for ad hoc networks (e.g. few disjoint paths or few splits). In this way, our solution is able to resist against passive attacks, even if a reasonable fraction of nodes are corrupted since we introduce asymmetric cryptography. However, even our approach requires more improvements and a complete validation, the first simulation results are interesting since they illustrate that we can improve and find an efficient trade-off between network performance and privacy protection. In this way, we enhanced some privacy principles and a method, that definitively should be implemented and compared to the simulations results.

Acknowledgment

We would like to acknowledge our partners from the DISCREET project. The DISCREET project was funded in part by the European Commission's Information Society Technology 6th Framework Programme. It started in December 2005 and will end in February 2008. For more information visit the project web site http://www.ist-discreet.org/.

References

[1] J. Liu, J. Kong, X. Hong, M. Gerla, “Performance Evaluation of Anonymous Routing Protocols in Mobile ad hoc Networks”, In IEEE Wireless Communications and Networking Conference (WCNC), Las Vegas, Nevada, USA, Apr. 3-6 2006.

[2] J. Kong, X. Hong, M. Gerla, M.Y. Sanadidi,”Comparison: ASR is a Variant of ANODR”, Technical report, UCLA, 2005.

[3] J. Kong, X. Hong,”ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile ad hoc Networks”, In ACM MOBIHOC’03, pages 291302, 2003.

[4] J. Kong, “Anonymous and Untraceable Communications in MobileWireless Networks”, PhD thesis, University of California, Los Angeles, June 2004.

[5] Denh Sy, Rex Chen and Lichun Bao, “ODAR: On-Demand Anonymous Routing in ad hoc Networks”, Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference, p267-276, Vancouver, Canada, October 2006

[6] D. Chaum. “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”. Communications of the ACM, Vol. 24 Number 2, Feb. 1981.

[7] M. J. Freedman, R. Morris. “Tarzan: A Peer-to-Peer Anonymizing Network Layer”. Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002). 2002.

[8] R. Dingledine, N. Mathewson, P. Syverson. “Tor: The Second-Generation Onion Router”. In Proc. of 13th Usenix Security Simposyum , August 2004.

[9] W. Lou, W. Liu, Y. Fang, “SPREAD: Improving network security by multi-path routing”, IEEE Milcom’03, Boston, MA, Oct 2003

[10] W. Luh and D. Kundur, “Distributed Privacy for Visual Sensor Networks via Markov Shares”, Proc. 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems, Columbia, Maryland, April 2006.

[11] M. Naor and B. Pinkas, “Oblivious Transfer and Polynomial Evaluation”, Proc. Of the 31st Symp. on Theory of Computer Science (STOC), Atlanta, GA, pp. 245-254, May 1-4, 1999.

[12] O. Goldreich, R. Rubinfeld and M. Sudan, “Learning polynomials with queries: the highly noisy case”, SIAM J. on Discrete Math., pp. 535–570, 2000.

[13] V.Guruswami and M.Sudan, “Improved decoding of Reed-Solomon and algebraic-geometry codes ,” IEEE Trans. on Information Theory, vol. 45, pp. 1757–1767, 1999.

[14] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory”, DSN Prog. Rep., Jet Prop. Lab, California Inst. Technol., Pasadena, CA, pp. 114–116, 1978.

[15] Claudia Diaz and Bart Preneel, “Reasoning about the Anonymity Provided by Pool Mixes that Generate Dummy Traffic”, Information Hiding. J. Fridrich (Ed.), Springer, LNCS 3200, pp. 309-325, 2004.

[16] Anja Jerichow, “Generalisation and security improvement of mixed-mediated anonymous communications”, PhD Thesis, Technischen Universitat Dresden, 2000.

[17] Raghav Bhaskar, Daniel Augot, Valerie Issarny and Daniele Sacchetti, “An Efficient Group Key Agreement Protocol for Ad hoc Networks”, IEEE Workshop on Trust, Security and Privacy in Ubiquitous Computing (A_liated with WoWMoM 2005), 12-16 June 2005, Taormina, Italy.

[18] Neal Koblitz, “Elliptic curve cryptosystems”, Mathematics of Computation 48, 1987, pp 203-209.

[19] Joan Daemen, Vincent Rijmen, “The block cipher Rijndael”, CARDIS 1998, LNCS 1820, pp. 247-256, 2000.

[20] OMNET++: http://www.omnetpp.org/.

[21] T. Clausen, P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, IETF, Request For Comment 3626, October 2003.