Provable Synthetic Coordinates for Increasing PoWs Effectiveness Against DoS and Spam

Marius Cristea

"Politehnica" University of Timisoara, Romania,
Email: cristea12@gmail.com

Bogdan Groza

"Politehnica" University of Timisoara, Romania,
Email: bogdan.groza@aut.upt.ro

***Abstract*—The effectiveness of synthetic coordinate systems against DoS and spam stems from the fact that, while changing or hiding a logical address is easier, changing the location of the spammer inside the network should be harder. But synthetic coordinate systems are limited by the fact that malicious nodes can easily lie about their position or introduce additional delays which have an immediate impact on it. For this purpose, we enhance the synthetic coordinate system provided by Vivaldi with secure nonces that are periodically broadcasted by trusted servers to achieve a provable location claim within the overlay network. As we advocate in this work, secure localization can help in choosing the hardness of PoWs since locations from which more malicious traffic originates can receive PoWs with higher difficulties.**

***Index Terms*—DoS, localization, spam, Vivaldi**

I. Introduction

Denial of Service (DoS) attacks and their distributed version (DDoS) are an important problem to network users and network service providers, causing disruption in communication at a very big scale. Email spam, or unsolicited emails, is an ever increasing phenomenon that costs industry in the order of billions of dollars according to some estimations. Up to this day, there is no perfect solution against such attacks and it seems that the only solution is to iteratively improve filters. In this spirit, we advocate here the use of secure source localization in order to increase the efficiency of spam detection and DoS mitigation. It is well known that it is not hard for an attacker to modify the address of a compromised host and it is also feasible to change the body of a message in such a way that it can trick even the most vigilant filter. On the other hand, finding new locations for attackers throughout the Internet should be harder. Usually attackers use botnets for spam or DoS delivery and these botnets are used repeatedly through time [3]. Thus we emphasize on the use of secure localization for a judicious choice on the amount of work used in PoW (Proof-of-Work) protocols.

In particular we use localization in an overlay network created using an enhanced Vivaldi algorithm [2] that assures secure localization. Several solutions for localization have been proposed in the literature. These solutions can be very simple, based on round trip time (RTT) measurement, or more advanced, based on RTT estimation. The solutions which use RTT estimation are known as virtual coordinates systems and can be either centralized ore decentralized. The idea of localizing DoS sources is not new. Usually packet tracing is used for such purpose but this is not always possible because of the different hops (between the attacker and the victim) that are under different security policies which may or not allow traceback. Regarding spam, in [5] the concept of Trust-by-Wire is introduced together with the IPclip mechanism which augments emails with location information that can be used for spam filtering together with other anti-spam mechanisms.

II. Secure Localization

By relying only on RTT for localization in the synthetic coordinates system, in Vivaldi a node can lie about its position and its local error [4]. To overcome this issues we proposed a replacement for RTT counting: instead of directly counting the RTT the nodes can use the distance function over rhythmically broadcasted nonces. Rhythmic nonces were introduced in [1] as a source for generating cryptographic puzzles to assure DoS resilience. A rhythmic nonce is defined as a number from a sequence, i.e., $(s_i) \in A^{\mathbb{N}}$, having the property that finding s_{i+1} from $s_i, s_{i-1}, ..., s_0$ is an intractable problem, and for every $k > 0$ there is an easy to compute function: $d_k(s_i, s_j) = min(|i - j|, k)$ called distance function.

Now, a new node N_a, who just entered the network, needs to listen to rhythmic nonces coming from any of the trusted rhythmic nonces servers (RNS) which are deployed in the network and their positions and local errors are publicly available through a public localization service (PLS). These servers are synchronized and are continuously updating their position using the same Vivaldi algorithm.

Self establishment of location. To establish its position, node N_a broadcasts ($\twoheadrightarrow$) a localization *request*. When receiving the request a RNS will send him back a window of w nonces $s_{i+1}, s_{i+2}, ..., s_{i+w}$. Further, N_a responds with a hash for each of the nonce $H(s_{i+1}), H(s_{i+2}), ..., H(s_{i+w})$. This communication takes place in an asynchronous mode ($\rightsquigarrow$). That is, RNS sends the nonces according to the scheduled delay and N_a responds as soon as he receives each nonce without waiting for the next one to arrive. We assumed that when the request arrives at RNS the most recently released nonce is s_i but RNS waits until the time for the next nonce comes, this will not cause a significant delay as nonces are released in the order of milliseconds and will improve the accuracy. When the window is finished, RNS computes the average round trip time

and sends N_a the distance $d(N_a, RNS)$. This protocol can be described as: 1. $N_a \twoheadrightarrow RNS : request$, 2. $RNS \rightsquigarrow N_a : s_{i+1}, ..., s_{i+w}$, 3. $N_a \rightsquigarrow RNS : H(s_{i+1}), ..., H(s_{i+w})$, 4. $RNS \rightarrow N_a : d(N_a, RNS), sig_{RNS}(d(N_a, RNS))$.

Having a fixed RNS, node N_a can intend to lie about its position but only by pretending to be further and not closer to RNS. Fig. 1 suggests this situation. If N_a pretends to be at position N'_a with $d' < d$, then RNS must receive s_i at the time when $s_{i+2d'}$ is released. However this will require N_a to send s_i at moment $i+2d'-d$ but he is not in possession of s_i at this time which arrives only at a later time $i+d$ (obviously $i+d > i+2d'-d$) and due to the security condition from the definition of the rhythmic nonces he cannot forge it either to send it sooner.

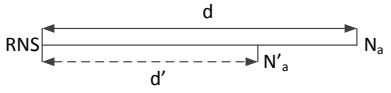

Fig. 1. Node N_a pretends that it's closer (N'_a) to RNS.

A. DoS resilience with SSL/TLS

We modify the protocol in such way that when a client wants to connect to a server it will send its position along with the request. After the server replies with ServerHello as usual and if it is under heavy load, the server will send the client's position to PLS in order to receive a list of 3 nonce servers that can triangulate the client. The server forwards this list to the client and the client will listen for nonces coming from the 3 nonces server dictated by the SSL server. After receiving the nonces the client will respond as described previously by the modified Vivladi algorithm. The nonce servers will verify the answers from the client and will inform the PLS about the validity of the client's position. The SSL server will request the validity of the client's position to PLS and after receiving the validity conformation, the server will calculate the difficulty of the PoW. The difficulty will depend on the number of requests arriving from the proximity of the client.

B. Email source localization

Email source localization can be achieved by introducing only some small changes to the existing SMTP protocol (Fig. 2). When a node or a client N_a wants to send an email it concatenates its location $\mathcal{P}(N_a)$ to the email (step 1). When receiving the email, the email server MS will consult the PLS (step 2) to obtain the id of three nonces (RNS_1, RNS_2, RNS_3) servers that form a triangle around the client (step 3). To verify if N_a pretends to be at a different position, MS will request N_a (step 4) to be verified by the three nonces servers (steps $5^k - 6^k, k = \overline{1,3}$) and will consult the PLS for the result (steps 8, 9). In this case an email can be marked as spam if it originates from a known malicious location or in a same manner as in the previous protocol a PoW can be added.

III. Conclusion

We believe that secure localization is an interesting option for combating spam and for increasing DoS resilience with proofs-of-work. Since there is no approach so far that works best against malicious traffic and this approach is not going to solve the problem either, we believe that it can be helpful as a new rule to existing filters or as calibration criteria for PoW protocols. It was our intention so far to make an account on the feasibility of such a solution, while experimental results in a real world network are subject of future work for us.

Acknowledgment

This work is partially supported by the strategic grant POSDRU/88/1.5/S/50783, Project ID50783 (2009), co-financed by the European Social Fund Investing in People, within the Sectoral Operational Program Human Resources Development 2007/2013.

References

[1] E. M. Chan, C. A. Gunter, S. Jahid, E. Peryshkin, and D. Rebolledo, "Using rhythmic nonces for puzzle-based dos resistance," in *Proceedings of the 2nd ACM workshop on Computer security architectures*, ser. CSAW '08. ACM, 2008, pp. 51–58. [Online]. Available: http://doi.acm.org/10.1145/1456508.1456518

[2] F. Dabek, R. Cox, F. Kaashoek, and R. Morris, "Vivaldi: a decentralized network coordinate system," in *Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, ser. SIGCOMM '04. ACM, 2004, pp. 15–26. [Online]. Available: http://doi.acm.org/10.1145/1015467.1015471

[3] O. Demir and B. Khan, "Finding ddos attack sources: Searchlight localization algorithm for network tomography," in *Proceedings of the 7th International Wireless Communications and Mobile Computing Conference*, ser. IWCMC '11. IEEE Press, 2011, pp. 418–423. [Online]. Available: http://dx.doi.org/10.1109/IWCMC.2011.5982570

[4] M. A. Kaafar, L. Mathy, T. Turletti, and W. Dabbous, "Virtual networks under attack: disrupting internet coordinate systems," in *Proceedings of the 2006 ACM CoNEXT conference*, ser. CoNEXT '06. ACM, 2006, pp. 12:1–12:12. [Online]. Available: http://doi.acm.org/10.1145/1368436.1368453

[5] H. Widiger, S. Kubisch, P. Danielis, J. Schulz, D. Timmermann, T. Bahls, and D. Duchow, "Ipclip: An architecture to restore trust-by-wire in packet-switched networks," in *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*. IEEE Computer Society, 2008, pp. 312 –319.

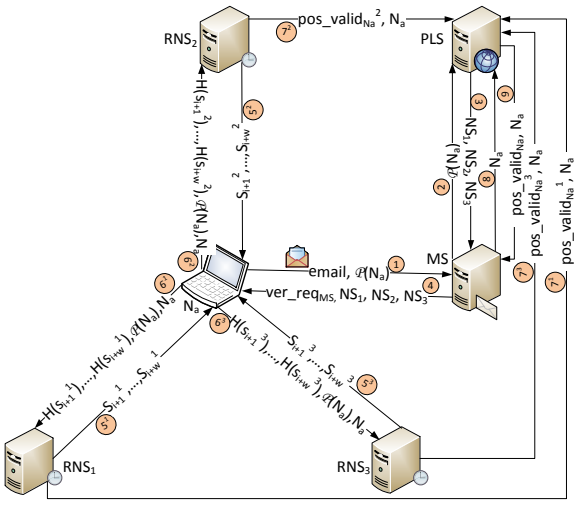

Fig. 2. Using the adapted Vivaldi algorithm to identify spam source location.