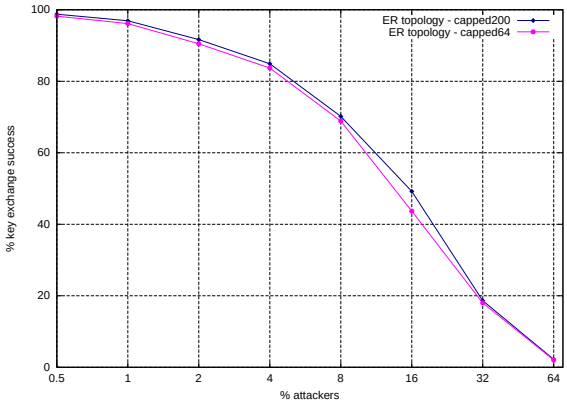

Figure 12. Influence of the maximum number of authorized hops.

and 200. We observe two curves that evolve similarly and are extremely close.

The number of hops has no significant influence on the success rate of the key exchange within the scope of the settings used in our experiments.

5.6. Influence of Routing Modes

We now discuss two modes of routing packets within the P2P network during a multipath key exchange process. In the *relax* mode, the process requires many disjoint paths that are relatively long. On the other hand, the *strict* mode corresponds to a reduced number of disjoint paths that are also short.

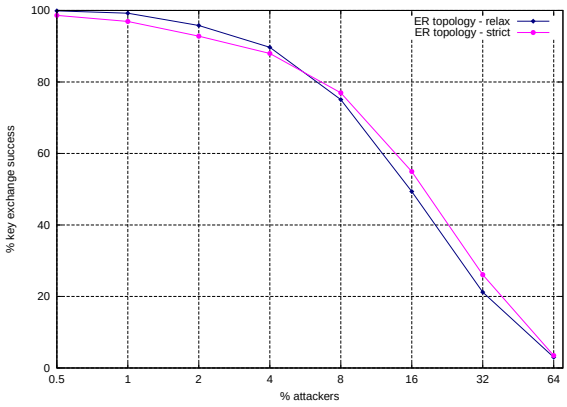

Figure 13. Comparison between the relax and strict routing modes.

Figure 13 depicts the results of our experiments in a network based on the ER topology. We observe that although the two curves are close, an interesting pattern emerges: for smaller proportions of attackers, the strict mode provides lower success rates for key exchange; for higher proportions of attackers, the relax mode is the one that leads to lower performances. This could be explained by the fact that when the number of attackers are small, a large number of paths (*relax mode*) increases the chance of avoiding them. On the other hand, when the number of attackers gets large, shorter paths (*strict mode*) are more effective.

Large numbers of disjoint paths and short paths favorably influence the success rates of the multipath key exchange scheme. The former works well in presence of small scale coordinated attacks while the latter is recommended for largely infected networks.

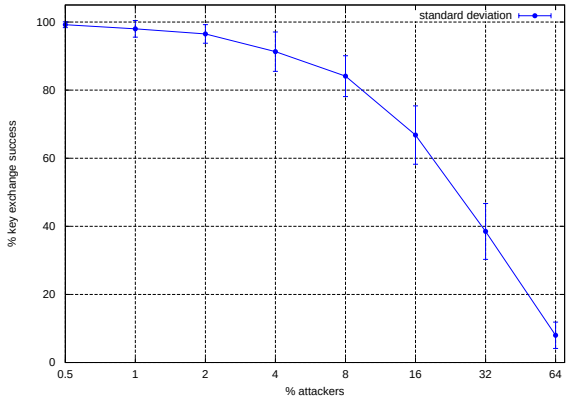

Figure 14. Standard deviation in the BGP-4 network map [17].

6. Security Analysis

In a multipath key exchange scheme, a malicious node that wishes to compromise a key being exchanged must be able to collect each of all key components routed over the network. Formally, when paths $\mathcal{P}_0, ..., \mathcal{P}_{k-1}$ are used to send several distinct subkeys from source $\mathcal{S}$ to destination $\mathcal{D}$, the only malicious nodes that could compromise the key should be located at the intersection of all paths. In other words, all the malicious node belong to set $M = \bigcap_{i=0}^{k} \mathcal{P}_i$ which represents the set of intersection points of all paths $\mathcal{P}_i$. $\mathcal{S}$ and $\mathcal{D}$ are obviously ignored in this set. Thus, when $\bigcap_{i=0}^{k} \mathcal{P}_i = \emptyset$ (*bigon criterion* is respected [11, Lemma 2.5]), then all paths are disjoint and any MITM attack attempt cannot succeed. In such a desirable case, there exists a k-connected subgraph between $\mathcal{S}$ and $\mathcal{D}$ in the network topology. When $|\bigcap_{i=0}^{k} \mathcal{P}_i| \geq 1$, there exists a real risk that MITM attacks will be committed on exchange transmitted between $\mathcal{S}$ and $\mathcal{D}$.

Consequently, the probability to have a MITM attack is estimated by $\sigma = \frac{|\bigcap_{i=0}^{k} \mathcal{P}_i|}{|\bigcup_{i=0}^{k} \mathcal{P}_i|}$ (where each path $\mathcal{P}_i$ is constituted of a set of consecutive hops from source $\mathcal{S}$ to destination $\mathcal{D}$). When all used paths are pairwise disjoint, the probability of *isolated* MITM attack (no *coordinated* MITM attack) is then: $\sigma = 0$ (i.e $|\bigcap_{i=0}^{k} \mathcal{P}_i| = 0$).

The number of distinct paths is also dependent on the source node degree. Thus, for a given *q-regular tree*, if q is a large number, then there is a probability to have several disjoint transmission channels. Nonetheless, despite the robustness of our multipath negotiation approach, cooperative (i.e., coordinated) MITM attacks, where several nodes maliciously cooperate to compromise a key, are possible. However, it is very hard, and excessively costly to execute such an attack in a real environment, especially in distributed systems where network topology changes dynamically.

In order to improve performances, re-authentication feature is introduced (see subsection 3.3). However, this challenge message used in this phase could be replayed. Furthermore, when a malicious node caches a challenge message, it can then create its copies and send them successively to target node. Thus, target node tries to resolves each challenge request because it does not know what packet is more fresh than other. Consequently, it will be rapidly saturated with requests from malicious node. Therefore, this causes a Denial-of-Service (DoS) attack.

In order to avoid such an attack from malicious nodes, a timestamp is assigned to each encrypted challenge message. Thus, the target node could distinguish between fresh packets and replayed packets.

Furthermore, during the key negotiation phase, all packets are exchanged in a clear text mode. Thus, traffic analysis attacks could reveal details about captured packets such as *sequence number* or *payload* which is nothing other than the transported subkey. Hence, multipath key exchange is needed to prevent the knowledge of all subkeys.

Figure 15 illustrates the slight decrease of key exchange success rate when the size of the network grows. In other words, the number of successful MITM attacks increases with the network size. As the number of attackers was set in our simulations to be proportional to the network size, this means that the size has indeed a small negative impact on the success rate. This is due to the consecutive average increase of the length of the paths themselves which increase their chance of being intercepted.

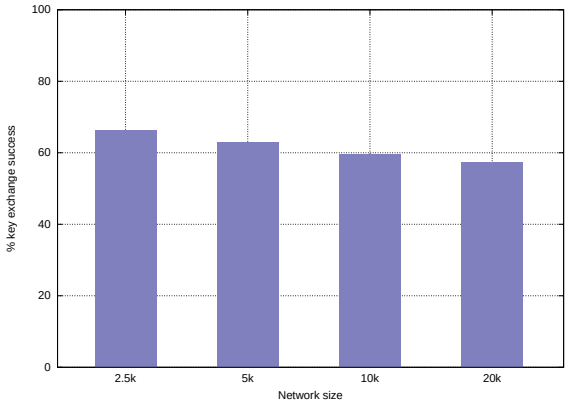

Figure 15. Variations of key exchange success rates for different network sizes (ER topology, capped by 64 hops max per path).

7. Related Work

Previous work have proposed several security infrastructures over fully decentralized or ad hoc networks [6, 7, 10, 15, 23, 27]. Although they are designed to be suitable in such environments, proposed approaches fulfill this gaol with more or less success and mostly with many caveats. In this section, we describe some models proposed in the literature to highlight the benefits of our approach.

Srivasta and Liu have relied on the Diffie-Hellman algorithm to deliver a solution that prevents threats in DHT networks [21]. Their scheme, however, remained sensitive to Man-in-the-middle attacks. Wang *et al.* have built a distributed PKI on top of the Chord structured overlay network [3]. They have used threshold cryptography to distribute the functionality of the PKI across the nodes of the DHT network. This Chord-PKI provides traditional PKI features such as certification, revocation, storage and retrieval.

Jiejun K. *et al.* propose to distribute certification authority functions through a threshold secret sharing mechanism [14]. In this system, private key is computed by k neighbor nodes and public key is derived from node identity.

Threshold cryptography is also used in identity-based key managements [7]. Nutshell, the key idea for identity-based cryptography is to define public keys derived from communicating nodes identities [20]. This method is really interesting however, the process of authentication could cause network overhead and the achieving of the value of threshold is not still guaranteed.

Takano *et al.* have designed a Multipath Key Exchange [23] similar to that proposed in our work. Their techniques however were designed to fit the Symphony and Chord P2P systems that are based upon

a ring topology. However, this inflexibility causes some drawbacks. Indeed, the proposed approach is based on clockwise/anticlockwise routing and this makes it sensitive to coordinated MITM attacks.

Jaydip Sen proposes a multipath certification protocol for MANETs that proceeds by broadcasting in order to discover the route between both source and destination nodes [19]. The key exchange protocol is based on this routing approach to retrieve the public keys of the nodes. However, broadcasting technique has proven that is not relevant in scalable networks such as fully decentralized P2P systems. Therefore,

Shehadeh E. *et al.* investigate secret key generation from wireless multipath channels [10]. The proposed protocol is based mainly on both the physical characteristics of the wireless channel and key predistribution schemes. This solution is implemented within physical layer.

8. Conclusion

P2P networks are self-organizing systems that do not need to resort to any central coordination point. The flexibility of such networks thus allows them to operate effectively on the Internet. Unfortunately, the inherent features that make them desirable also make them vulnerable to various security threats such as eavesdropping, modification and usurpation attacks.

In order to address the security challenges of P2P networks, we propose an improvement built upon our CLOAK architecture defined in our previous work [25] on one hand and a new approach for key exchange that generalizes a model proposed by Takano *et al.* [23] on the other hand. The benefit of using CLOAK instead of another DHT is that it does not use routing tables and does not impose any topology structure upon its peers. Our solution presented in this paper allows two peers from a P2P network to generate a common secret key in order to secure their communication without the need of a trusted third party when multipath is possible. This key generation is based on the Diffie-Hellman method with several subkeys being exchanged through several disjoint paths. Simulation results show that the probability of securely generating a key is above 90% when the percentage of coordinated attackers is lower than 2%. Depending on the topology type, the network size and the amount of attackers, the success rate can remain around 80% when the percentage of coordinated attackers is around 4%. As the size of P2P networks is typically several orders of magnitude (from thousands to millions of nodes), we expect our solution to be efficient because a few percent of coordinated attackers will result in hundreds of those attackers being needed in the network and that may not be feasible in practice.

For future work, we will consider adding peer authentication which for the moment only relies on the CLOAK DHT not allowing a peer to usurp another peer's name. We will also evaluate the time which is necessary to exchange a key. Although this happens only at the beginning of the communication and needs not be done after that even when interruptions happen, we will use event driven temporal simulations for investigating those delays.

References

[1] Daouda Ahmat, Tegawende Bissyande, and Damien Magoni. Towards securing communications in infrastructure-poor areas. In *5th EAI International Conference on e-Infrastructure and e-Services for Developing Countries*, 2013.

[2] Daouda Ahmat and Damien Magoni. Muses: Mobile user secured session. In *5th IFIP Wireless Days Conference*, pages 1–6, 2012.

[3] Agapios Avramidis, Panayiotis Kotzanikolaou, Christos Douligeris, and Mike Burmester. Chord-pki: A distributed trust infrastructure based on p2p networks. *Comput. Netw.*, 56(1):378–398, January 2012.

[4] Thomas Bohme, Frank Goring, and Jochen Harant. Menger's theorem. *Journal of Graph Theory*, 37(1):35–36, 2001.

[5] Cyril Cassagnes, Telesphore Tiendrebeogo, David Bromberg, and Damien Magoni. Overlay addressing and routing system based on hyperbolic geometry. In *Proceedings of the 16th IEEE Symposium on Computers and Communications*, pages 294–301, 2011.

[6] Miguel Castro, Peter Druschel, Ayalvadi Ganesh, Antony Rowstron, and Dan S. Wallach. Secure routing for structured peer-to-peer overlay networks. *SIGOPS Oper. Syst. Rev.*, 36(SI):299–314, December 2002.

[7] Hongmei Deng, Anindo Mukherjee, and Dharma P. Agrawal. Threshold and identity-based key management and authentication for wireless ad hoc networks. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 2 - Volume 2*, ITCC '04, pages 107–, Washington, DC, USA, 2004. IEEE Computer Society.

[8] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[9] Antonio Gracia Dimitri Defigueiredo and Bill Kramer. Analysis of peer-to-peer network security using gnutella, 2002.

[10] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe. Towards robust key extraction from multipath wireless channels. *Communications and Networks, Journal of*, 14(4):385–395, 2012.

[11] D. B. A. Epstein. Curves on 2-manifolds and isotopies. In *Acta Math*, pages 15–16, 1966.

[12] Paul Erdős and Alfred Rényi. On the evolution of random graphs. *Publications of the Mathematical Institute of the Hungarian Academy of Sciences 5*, pages 17–61, 1960.

[13] Ken ichi Kawarabayashi, Yusuke Kobayashi, and Bruce A. Reed. The disjoint paths problem in quadratic time. *J. Comb. Theory, Ser. B*, 102(2):424–435, 2012.

[14] Jiejun Kong, Z. Petros, Haiyun Luo, Songwu Lu, and Lixia Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Network Protocols, 2001. Ninth International Conference on*, pages 251–260, 2001.

[15] Hyeokchan Kwon, Sunkee Koh, J. Nah, and Jongsoo Jang. The secure routing mechanism for dht-based overlay network. In *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on*, volume 2, pages 1300–1303, 2008.

[16] Damien Magoni and Jean-Jacques Pansiot. Internet topology modeler based on map sampling. In *Proceedings of the 7th IEEE Symposium on Computers and Communications*, pages 1021–1027, 2002.

[17] Y. Rekhter. A border gateway protocol 4 (bgp-4). *RFC 4271*, http://www.ietf.org/rfc/rfc4271.txt ,january, 2006.

[18] J. Schafer and K. Malinka. Security in peer-to-peer networks: Empiric model of file diffusion in bittorrent. In *Internet Monitoring and Protection, 2009. ICIMP '09. Fourth International Conference on*, pages 39–44, 2009.

[19] J. Sen. A multi-path certification protocol for mobile ad hoc networks. In *Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference on*, pages 1–4, 2009.

[20] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[21] M. Srivatsa and Ling Liu. Vulnerabilities and security threats in structured overlay networks: a quantitative analysis. In *Computer Security Applications Conference, 2004. 20th Annual*, pages 252–261, 2004.

[22] Jani Suomalainen, Anssi Pehrsson, and Jukka K. Nurminen. A security analysis of a p2p incentive mechanisms for mobile devices. In *3rd International Conference on Internet and Web Applications and Services*, pages 397–402, 2008.

[23] Y. Takano, N. Isozaki, and Y. Shinoda. Multipath key exchange on p2p networks. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, pages 8 pp.–, 2006.

[24] T. Tiendrebeogo, D. Ahmat, and D. Magoni. Reliable and scalable distributed hash tables harnessing hyperbolic coordinates. In *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, pages 1–6, 2012.

[25] Telesphore Tiendrebeogo, Daouda Ahmat, Damien Magoni, and Oumarou Sié. Virtual connections in p2p overlays with dht-based name to address resolution. *International Journal on Advances in Internet Technology*, 5(1):11–25, 2012.

[26] Guido Urdaneta, Guillaume Pierre, and Maarten Van Steen. A survey of dht security techniques. *ACM Comput. Surv.*, 43(2):8:1–8:49, February 2011.

[27] Peng Wang, Ivan Osipkov, and Yongdae Kim. Myrmic: Secure and robust dht routing. Technical report, University of Minnesota, 2007.