Analysis of Qos Aware Cloud Based Routing for Improved Security

Rahul pethe[1]* g. M. Asutkar[2] s. M. Asutkar[3]

[1]Assistant Professor, Priyadarshini Institute of Engineering and Technology, Nsgpur, Maharashtra, India

[2]Vice-Principal, Priyadarshini Institute of Engineering and Technology, Nsgpur, Maharashtra, India

[3] Associate Professor, MIET, Gondia, Maharashtra, India

* rahul2480@gmail.com

Abstract: The recent advances and the convergence of micro electro-mechanical systems technology, integrated circuit technologies, microprocessor hardware and Nano-technology, wireless communications, Ad-hoc networking routing protocols, distributed signal processing, and embedded systems have made the concept of Wireless Sensor Networks (WSNs). Sensor network nodes are limited with respect to energy supply, restricted computational capacity and communication bandwidth. Most of the attention, however, has been given to the routing protocols since they might differ depending on the application and network architecture. To prolong the lifetime of the sensor nodes, designing efficient routing protocols is critical. Even though sensor networks are primarily designed for monitoring and reporting events, since they are application dependent, a single routing protocol cannot be efficient for sensor networks across all applications. In this paper, we analyze the design issues of sensor networks and present a classification and comparison of routing protocols. This comparison reveals the important features that need to be taken into consideration while designing and evaluating new routing protocols for sensor networks. A reliable transmission of packet data information, with low latency and high energy-efficiency, is truly essential for wireless sensor networks, employed in delay sensitive industrial control applications. The proper selection of the routing protocol to achieve maximum efficiency is a challenging task, since latency, reliability and energy consumption are inter-related with each other. It is observed that, Quality of Service (QoS) of the network can improve by minimizing delay in packet delivery, and life time of the network, can be extend by using suitable energy efficient routing protocol.

Keywords: Anonymity, Qos, Cloud, Security, K-Copy, Aggregation

Introduction

Routing is one of the critical technologies in WSNs. Opposed to traditional *ad hoc* networks, routing in WSNs is more challenging as a result of their inherent characteristics [3,4]. Firstly, resources are greatly constrained in terms of power supply, processing capability and transmission bandwidth. Secondly, it is difficult to design a global addressing scheme as Internet Protocol (IP). Furthermore, IP cannot be applied to WSNs, since address updating in a large-scale or dynamic WSN can result in heavy overhead. Thirdly, due to the limited resources, it is hard for routing to cope with unpredictable and frequent topology changes, especially in a mobile environment. Fourthly, data collection by many sensor nodes usually results in a high probability of data redundancy, which must be considered by routing protocols. Fifthly, most applications of WSNs require the only communication scheme of many-to-one, *i.e.*, from multiple sources to one particular sink, rather than multicast or peer to peer. Finally, in time-constrained applications of WSNs, data transmissions should be accomplished within a certain period of time. Thus, bounded latency for data transmissions must be taken into consideration in this kind of applications. Nevertheless, energy conservation is more important than quality of service (QoS) in most applications in that all sensor nodes are constrained with energy which is directly related to network lifetime.

1. Literature review

Mixnet-based conventions demonstrate the most heterogeneous directing plan. The primary explanation behind this is they exhibit steering assorted variety on numerous directing structure squares, for example, proposing dissimilar flushing systems, separating hub choice procedures, which thus lead to topological contrasts. As referenced before, existing directing systems can be characterized into free-courses blend systems and blend falls. Be that as it may, we recognize whether an association is possibly permitted between two hubs or not founded on steering of the messages. Consequently, we stamped the majority of the blend course arranges as completely associated and just Webmixes and Restricted steered blend organizes as somewhat associated. As a rule, blend course arranges utilize rather synchronized association since messages are sent in groups and for the most part rely upon their flushing calculations in an opportune calendar. For instance, planned blends lead to synchronized message transmission. Review that the flushing calculation in Mixmaster and Mixminion mostly utilizes time confinements. In any case, we consider these two conventions with offbeat message transmissions because of the likelihood that low traffic may prompt an edge limitation rather than a period confinement. With respect to free-course frameworks, in SG-blends, message transmission are additionally synchronized because of doled out time extends by the directing initiator. In any case, these planning ranges are not facilitated with different clients or blend hubs. Dingledine et al's. proposition for a notoriety framework for mixnets [1] likewise utilizes a synchronized message handing-off to empower checking the accuracy of the directing procedure. In the blend conventions, hub the executives has not been constantly indicated in the convention portrayal. For instance, in Chaumian blends, the perspective on the directing chief isn't talked about; in any case, it very well may be certainly found that it is finished. The mysterious remailer Mixmaster does not talk about hub the executives either; in any case, the later usage utilizes specially appointed frameworks, which proposes a fractional view [2]. The remailer Mixminion characterizes a hub the board technique to guarantee a total view for the directing leader. Source-steering is one of the natural directing highlights of blend course conventions in light of the fact that the steering ways are fixed heretofore. Picking the blends for the blend course may be either deterministic, for example, on account of Webmixes or non-deterministic, for example, on account of Reliable blend falls. Flushing calculations do clearly affect booking. Note that a few conventions use haphazardness in the booking procedure (e.g., pool blends). Thusly, a few messages are sent later than others. Since individual messages don't have needs without anyone else, we classified them additionally as reasonable. How the arrangement of hubs is determined for hub choice has likewise not been indicated absolutely for blend systems. Similar holds for choice likelihood, for example, for Chaumian blends. For blend systems, we arranged the choice likelihood as deterministic on the grounds that all blends are picked for a solitary blend course. For both blend course conventions and free-course blend organizes, the determination set fluctuates relying upon the use of the AC arrange and on the potential secrecy properties. As referenced in Section Ⅲ-An, in blend falls, the choice likelihood has two measurements when more than one course exists. For example, Webmixes can give different blend falls, where blends are picked by the system director for each blend course. From there on, the client physically chooses one of these blend falls for steering her messages. Another blend course convention, where blends are chosen deterministic, is ISDN blends. All blend course conventions are high inactivity AC arranges and have a message-based correspondence mode; special cases are ISDNs, Real-time blends, and Webmixes, which are intended for low-inertness applications, for example, web perusing. Note that the latencies may be limited, for example if there should be an occurrence of Stop-and-go blends, where the postponements are arbitrarily chosen from a confined time extend. Onion steering conventions are all Tor related plans and thus, show the most homogeneous directing structure among the four examined convention classes. On a calculated dimension, every one of these conventions is similarly portrayed by their directing highlights. In any case, there are three special cases that effect: the fulfilment of the system see, the decency of booking, and the hub determination likelihood (leaving separated the nontechnical inquiry if the code has been made freely accessible). Their disparities, in any case, regularly lie in execution subtleties, which are not really pertinent to directing, for example, lessening cushion estimate [3]. Likewise, contrasts in the directing strategy, which don't change the steering highlight on a theoretical dimension, for example, changing hub choice probabilities [4] and [5], are similarly ordered in the table, however hub determination probabilities could be extraordinary. One innate directing element of onion steering conventions, due to keeping extra inactivity, is to have no synchronization, which makes such conventions delicate to timing assaults and worldwide enemies. Another inborn component is that all onion directing conventions have a customer server display, which improves their convenience and prompts a higher number of clients, consequently adding to better obscurity for onion steering conventions [6]. They are portrayed as total system see because of a focal expert, which appropriates the rundown of Tor switches. One special case is [7], which acknowledges private hub recovery and accordingly compels the chief's perspective on the system. A total view helps against foe biasing hub choice and is favoured in source-steering so as to keep the chief to look over a littler arrangement of hubs. Further inalienable directing highlights concerning the correspondence display incorporate steering type, planning, determinism in the hub determination, and the choice set. The special cases here are [8], [9], where they recommend a prioritization at the booking stage for intelligent traffic so as to decrease defers that intuitive clients may understanding. Hub determination in all onion directing based conventions is non-deterministic. This is imperative since the Tor arrange comprises of volunteers and it is in all respects prone to have a small amount of vindictive hubs among them. A nondeterministic hub determination diminishes the odds of reliably choosing noxious hubs. Since the enemy is thought to be neighbourhood, a non-deterministic hub determination makes focused on observation harder. Moreover, the hub choice likelihood is commonly weighted utilizing static parameters, with the exception of a couple of methodologies that powerfully alter loads, e.g., for adjusting security versus execution [10] and for maintaining a strategic distance from blockage [11], [12]. Onion steering conventions are low latency and have circuit-based correspondence mode, which are both inborn directing highlights of these conventions. Despite the fact that we characterize Tor as a convention where the steering leader has a total view, it merits referencing that the unlisted transfers, known as scaffolds, are not part of this view. Next, we talk about irregular walk conventions and DHT based conventions. Groups are Morphmix are two of the early irregular walk conventions that were proposed for mysterious correspondence. In any case, they present reasonable contrasts as far as directing highlights. The two Crowds and Morphmix have completely associated topologies since each hub may manufacture an association with each other hub, bringing about better accessibility of the framework, which prompts a greater assault surface for timing assaults. The way length in Crowds may fluctuate and is resolved in a non-deterministic way to make straightforward planning assaults more earnestly for outside, nearby, and aloof foes. In any case, this does not really hold for the case that somewhere around one of the hubs in the way is vindictive. In Morphmix, the initiator does not choose the hubs of the course herself, rather settles on the quantity of hubs and builds up the association. Groups is semi-decentralized in light of the fact that steering data of hubs is appropriated by a focal substance (the blender), which presents a solitary purpose of disappointment regarding hub organization. Morphmix, be that as it may, has a completely decentralized structure. The system see is finished in Crowds, which, from one viewpoint, shields Crowds from obscuration assaults and then again, is essential since Crowds has a bounce by-jump directing sort that makes the hub choice delicate to be one-sided by foes. In Morphmix, the system see is halfway, and along these lines, witnesses were acquainted with keep the one-sided hub choice. In addition, an inalienable element of irregular walk conventions is that the hub determination is nondeterministic. In Crowds, every hub is browsed the arrangement of all hubs dependent on a geometric conveyance [13]; while, in Morphmix, the initiator knows a subset of hubs. An inborn steering highlight of DHT-based conventions is halfway associated topology and an incomplete system see. The steering data is appropriated among hubs and no single hub has the total rundown. Such a plan expands the adaptability of the conventions. A halfway associated system topology makes DHT-based conventions less flexible against DoS assaults, which go for disengaging the system however much as could be expected contrasted with onion steering conventions. The association course is bidirectional for most of conventions with two exemptions. The special cases are the document sharing applications Gnunet and Freenet Opennet mode. For the most part, DHT-based conventions are completely distributed conventions. There are two special cases in this classification: in particular, Torsk and Salsa, where the first has a half and half job structure while the last one permits both cross breed and completely distributed job structures. For being halfway associated, DHT-based conventions give a fractional perspective on the system to the steering chief. Note this may present a progression of assaults. Instances of assaults against conventions that give just a fractional perspective on the system to the directing leader are course fingerprinting assaults [14], and course connecting assaults [15]. Another arrangement of assaults, which may be conceivable because of an incomplete system see, are assaults that go for disengaging target hubs from whatever is left of the system, for example, overshadow assaults [16]. The majority of the DHT-based conventions are portrayed with a jump by-bounce directing sort. Special cases are NISAN, Salsa, and Octopus, with source-directing. In Octopus, there are two chiefs for hub choice; the way initiator who chooses just about a portion of the way and the last hub of that fragment, which starts whatever is left of the way. In our investigation, we couldn't discover much data about the booking of DHT-based conventions, specifically for conventions that have not been sent. The vast majority of the DHT-based conventions have nondeterministic hub determination; again here special cases are the document sharing applications, where the directing way shouldn't be unknown. The set choice for DHT-based conventions is, as a rule, all hubs inside the directing table (i.e., all hubs accessible to the leader). Be that as it may, there are two special cases:

2. Security optimization with the help of the k-copy cloud based protocol

Our routing algorithm can be depicted as follows,

- Deploy a system of N hubs put arbitrarily in a zone of x Y sq. meters
- Select any source (S) and goal (D) from the system for directing procedure
- Let the euclidean separation between hub S and D be dref
- Select all hubs from the system, where the accompanying conditions are fulfilled,
    - dsn+dnd > dref
    - dsn < dref
    - dnd < dref

where, dsn = Distance between source to chosen hub

dnd = Distance between chosen hub to goal

- This channels in just those hubs which are in the steering way, and evacuates every single other hub
- For every hub in the way, assess the accompanying measurement,

    Metric = di/Ei

    where, di = Distance between the hubs

    Ei = Energy of the source hub

- Start the hub choice from the source till the goal hub is come to. Once came to, send the information on the chose way
- Before sending the information, apply information accumulation at the source hub
- Split the amassed information into k parts, where k is the quantity of channels accessible for directing
- Send the information on all the k channels from the source hub to the goal
- Repeat this procedure for all interchanges

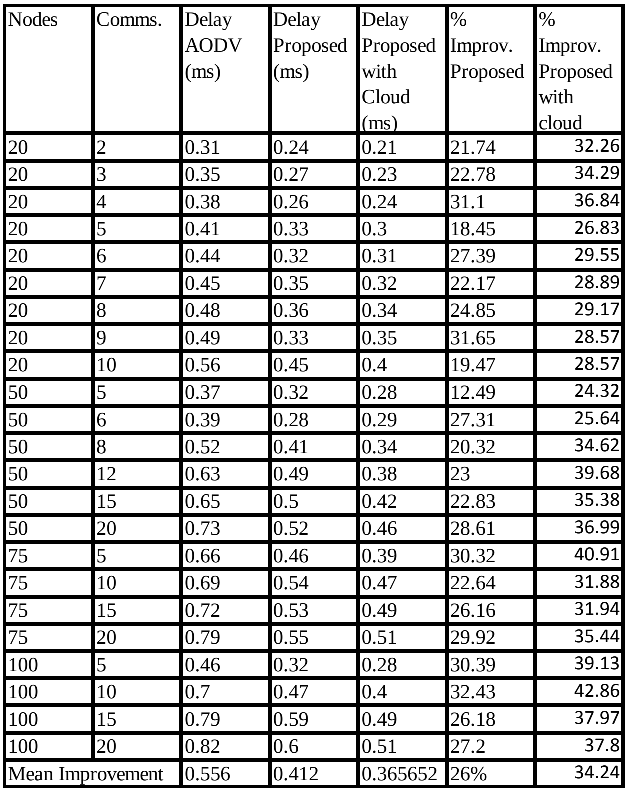
The above calculation ensures that the information is sent from the source to goal with least postponement, and least vitality because of information total, multichannel correspondence and consolidation of d/E factor in the steering procedure. The throughput is upgraded also because of progress in postponement and diminished parcel misfortune due to multichannel correspondence. This ensures the parcel is transmitted in the practically same planning interim as the past bundles, consequently decreasing the jitter of the system. The detailed result analysis is mentioned in the next section.

3. Results and Analysis

We simulated our routing protocol in the network simulator version 2.34 environment, under the following network conditions,

Network parameter	**Value**
Network type	Wireless
Number of nodes	30 to 100
Network area	300m x 300m
Routing protocols	QoS aware
Packet size	1000 bits @ 0.001 packets per second
Number of communications	2 to 20
Initial node energies	Randomized, with maximum energy of 1000 mJ per node
Energy model	2 mJ per transmission 1 mJ per reception 0.1 mJ idle energy

We compared our proposed protocol with the AODV routing for the wireless network, and the following parameters were obtained,



Nodes	Comms.	Delay AODV (ms)	Delay Proposed (ms)	Delay Proposed with Cloud (ms)	% Improv. Proposed	% Improv. Proposed with cloud
20	2	0.31	0.24	0.21	21.74	32.26
20	3	0.35	0.27	0.23	22.78	34.29
20	4	0.38	0.26	0.24	31.1	36.84
20	5	0.41	0.33	0.3	18.45	26.83
20	6	0.44	0.32	0.31	27.39	29.55
20	7	0.45	0.35	0.32	22.17	28.89
20	8	0.48	0.36	0.34	24.85	29.17
20	9	0.49	0.33	0.35	31.65	28.57
20	10	0.56	0.45	0.4	19.47	28.57
50	5	0.37	0.32	0.28	12.49	24.32
50	6	0.39	0.28	0.29	27.31	25.64
50	8	0.52	0.41	0.34	20.32	34.62
50	12	0.63	0.49	0.38	23	39.68
50	15	0.65	0.5	0.42	22.83	35.38
50	20	0.73	0.52	0.46	28.61	36.99
75	5	0.66	0.46	0.39	30.32	40.91
75	10	0.69	0.54	0.47	22.64	31.88
75	15	0.72	0.53	0.49	26.16	31.94
75	20	0.79	0.55	0.51	29.92	35.44
100	5	0.46	0.32	0.28	30.39	39.13
100	10	0.7	0.47	0.4	32.43	42.86
100	15	0.79	0.59	0.49	26.18	37.97
100	20	0.82	0.6	0.51	27.2	37.8
Mean Improvement		0.556	0.412	0.365652	26%	34.24

Similar comparisons were made for energy, packet delivery ratio, throughput and jitter. The following table shows the performance comparison for all the 5 parameters,

Parameter	AODV	Proposed	Proposed with cloud	% Improvement	% Improvement with cloud
Avg. Delay (ms)	0.556	0.412	0.351	26%	36.87
Avg. Energy (mJ)	3.126	2.198	1.963	29%	37.2
Avg. PDR (%)	99.5	98.6	99.2	0%	0.3
Avg. Throughput (kbps)	137.8	134.9	136.7	-0.50%	0.8
Avg. Jitter (ms)	0.0062	0.0058	0.006	7%	3.23

From the above table we can see that the system delay has been limited (also can be shown from the graph), the vitality utilization has been decreased by keeping up a consistent normal bundle conveyance proportion and normal throughput.

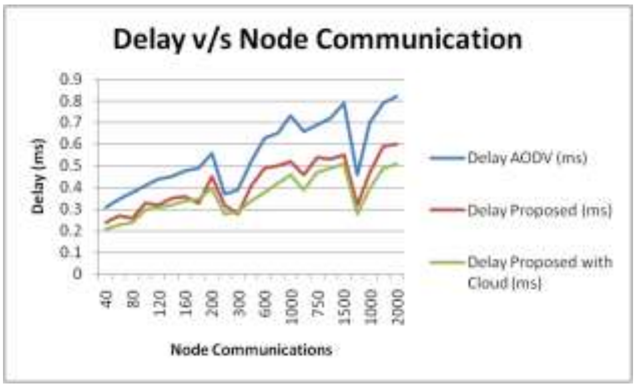


Figure 1: Delay v/s Number of communications

The general parcel conveyance jitter has likewise been marginally improved utilizing the AI approach. The postponement is decreased because of determination of least separation hubs for steering, while vitality is diminished in view of its consideration in the directing measurement as a conversely relative parameter. Because of decrease in postponement, the jitter is likewise diminished and along these lines it makes the system progressively dependable and predictable as far as parcel conveyance times at the collector. The PDR and throughput of AODV is as of now enhanced, and hence there in insignificant extent of progress around there. Also the security aspects of the research are improved with the help of the k-copy scheme as the data is more securely visible from source to destination without being compromised in the route.

The improvement of the parameters can also be visualized from the following graph,

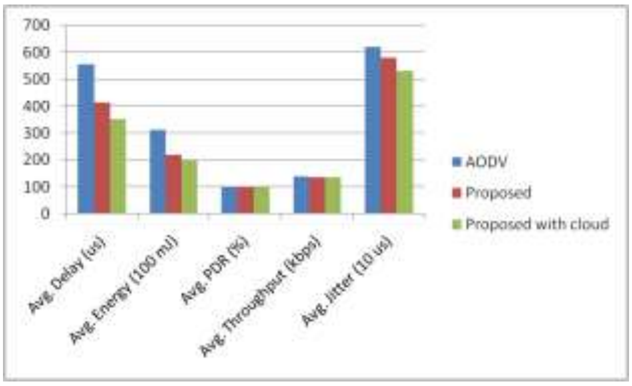


Figure 2: Comparison of all parameters

As we can see all parameters are either optimized or are almost similar as compared to the existing standard protocol. We prescribe scientists to additionally assess this AI directing system so as to check it's feasibility for the applications for which they would plan the correspondence arrange.

4. Conclusion

The proposed methodology when connected to the remote system gives a critical improvement in system execution, when contrasted and the on-going accepted AODV steering calculation. The execution improvement to arrange lifetime is over 25%, while the postpone minimization is over 20% for a wide assortment of system recreation parameters. This makes the system throughput decrease by a minuscule rate which is allowable by the remote systems, because of the way that our calculation builds the vitality utilization proficiency for the system that can be utilized viably by low power gadgets.

5. Future work

As a future work, we plan to realize the protocol using hardware implementation in a real time wireless based network, due to the low cost nature of Arduino based wireless nodes, the hardware realization can be done in a closed lab environment. We also intend to research more into the QOS improvement of the wireless networks by incorporating more parameters into our machine learning protocol, and also adding Q-Learning and deep nets into the routing algorithm, which can adapt to the network patterns and select the most optimum route intelligently and in real time, with minimum on-the-fly complexity.

References

1. A. Pfitzmann and M. Waidner, "Systems without client discernibleness - structure choices," in Advances in Cryptology - EUROCRYPT '85 (F. Pichler, ed.), vol. 219 of Lecture Notes in Computer Science, pp. 245–253, Springer Berlin Heidelberg, 1986.

2. B. Levine, M. Reiter, C. Wang, and M. Wright, "Timing assaults in low-dormancy blend frameworks," in Financial Cryptography (A. Juels, ed.), vol. 3110 of Lecture Notes in Computer Science, pp. 251– 265, Springer Berlin Heidelberg, 2004.

3. J. Kleinberg, "The little world wonder: An algorithmic viewpoint," in Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing, STOC '00, pp. 163– 170, ACM, 2000.

4. P. Mittal, F. Olumofin, C. Troncoso, N. Borisov, and I. Goldberg, "PIR-Tor: Scalable unknown correspondence utilizing private data recovery," in Proceedings of the twentieth USENIX Conference on Security, SEC '11, (Berkeley, CA, USA), pp. 31– 31, USENIX Association, 2011.

5. G. Danezis, "Measurable exposure assaults," in Security and Privacy in the Age of Uncertainty, IFIP TC11 eighteenth International Conference on Information Security (SEC '03), May 26-28, 2003, Athens, Greece, pp. 421– 426, 2003.

6. S. Goel, M. Robson, M. Polte, and E. Sirer, "Herbivore: A versatile and proficient convention for unknown correspondence," tech. rep., Cornell University, 2003.

7. D. I. Wolinsky, H. Corrigan-Gibbs, B. Portage, and A. Johnson, "Adaptable unknown gathering correspondence in the anytrust show," in European Workshop on System Security (EuroSec), vol. 4, 2012.

8. S. Roos, B. Schiller, S. Programmer, and T. Strufe, "Estimating freenet in the wild: Censorship-flexibility under perception," in Privacy Enhancing Technologies - fourteenth International Symposium, PETS 2014, Amsterdam, The Netherlands, July 16-18, 2014. Procedures, pp. 263– 282, 2014.

9. C. Tang and I. Goldberg, "An improved calculation for Tor circuit booking," in Proceedings of the seventeenth ACM Conference on Computer and Communications Security, CCS '10, (New York, NY, USA), pp. 329– 339, ACM, 2010.

10. S. Dolev and R. Ostrobsky, "Xor-trees for effective unknown multicast and gathering," ACM Trans. Inf. Syst. Secur., vol. 3, pp. 63– 84, May 2000.

11. R. Dingledine and P. Syverson, "Solid MIX course organizes through notoriety," in Financial Cryptography (M. Burst, ed.), vol. 2357 of Lecture Notes in Computer Science, pp. 253– 268, Springer Berlin Heidelberg, 2002.

12. J. Bos and B. nook Boer, "Location of disrupters in the dc convention," in Advances in Cryptology - EUROCRYPT '89 (J.- J. Quisquater and J. Vandewalle, eds.), vol. 434 of Lecture Notes in Computer Science, pp. 320– 327, Springer Berlin Heidelberg, 1990.

13. M. Waidner, "Unlimited sender and beneficiary untraceability disregarding dynamic assaults," in Advances in Cryptology - EUROCRYPT '89 (J.- J. Quisquater and J. Vandewalle, eds.), vol. 434 of Lecture Notes in Computer Science, pp. 302– 319, Springer Berlin Heidelberg, 1990.

14. D. I. Wolinsky, H. Corrigan-Gibbs, B. Portage, and A. Johnson, "Dispute in numbers: Making solid obscurity scale," in Proceedings of the tenth USENIX Conference on Operating Systems Design and Implementation, OSDI '12, pp. 179– 192, USENIX Association, 2012.

15. M. AlSabah, K. S. Bauer, T. Elahi, and I. Goldberg, "The way less voyaged: Overcoming Tor's bottlenecks with traffic part," in Privacy Enhancing Technologies - thirteenth International Symposium, PETS 2013, Bloomington, IN, USA, July 10-12, 2013. Procedures, pp. 143– 163, 2013.

16. M. Waidner and B. Pfitzmann, "The eating cryptographers in the disco: Unconditional sender and beneficiary untraceability with computationally secure usefulness," in Advances in Cryptology - EUROCRYPT '89 (J.- J. Quisquater and J. Vandewalle, eds.), vol. 434 of Lecture Notes in Computer Science, pp. 690– 690, Springer Berlin Heidelberg, 1990.

17. P. Golle and A. Juels, "Eating cryptographers returned to," in Advances in Cryptology - EUROCRYPT '04 (C. Cachin and J. Camenisch, eds.), vol. 3027 of Lecture Notes in Computer Science, pp. 456– 473, Springer Berlin Heidelberg, 2004.

18. O. Berthold, H. Federrath, and M. K ¨ohntopp, "Venture namelessness and imperceptibility in the web," in Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions, CFP '00, (New York, NY, USA), pp. 57– 65, ACM, 2000.

19. P. Wang, I. Osipkov, N. Container, and Y. Kim, "Myrmic: Provably secure and effective DHT steering," tech. rep., DTC, 2006.

20. O. Berthold, H. Federrath, and S. K ̈opsell, "Web MIXes: A framework for unknown and imperceptible web access," in Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, USA, July 25-26, 2000, pp. 115– 129, 2000.

21. R. Dingledine, M. Freedman, D. Hopwood, and D. Molnar, "Areputation framework to build MIX-Net dependability," in Information Hiding (I. Moskowitz, ed.), vol. 2137 of Lecture Notes in Computer Science, pp. 126– 141, Springer Berlin Heidelberg, 2001.

22. K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. More debilitated, "Low-asset steering assaults against Tor," in Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, WPES '07, (New York, NY, USA), pp. 11– 20, ACM, 2007.

23. M. K. Reiter and A. D. Rubin, "Groups: Anonymity for web exchanges," ACM Trans. Inf. Syst. Secur., vol. 1, pp. 66– 92, November 1998.