Eliminating the Requirement of IP Traceback with the Physical Layer on Quantum Networks

Qianhua Gao, Sangsig Kim, James G. Schiiller, and Huirong Fu
{qgao2, skim2345, fjgschiil, fu}@oakland.edu

***Abstract*—As the Internet becomes increasingly important as a business infrastructure, the number of attacks on it, especially denial-of-service attacks, IP spoofing, and other attacks requiring IP traceback continue to grow. To the offender, there is low risk of being caught and high opportunity to launch their attacks resulting in, for some companies alone, costs estimated at billions of dollars each year. This paper will explore a new scheme capable of eliminating the security threats of today requiring IP traceback, by seeking new methods to approach the problem. In the process, an entirely new solution was derived by extracting strategies learned from existing proposed schemes in conjunction with the writers' own ideas, namely private quantum channels, into what is called quantum network overlay.**

***Index Terms*—Quantum theory, computer network security, communication system security, data security, IP trackback, quantum private channel, quantum network overlay.**

I. Introduction

THE basic goal of this work is to propose a new scheme for IP traceback based on future networks. The quality of the new scheme should satisfy modern standard metrics used to evaluate the quality of previously proposed schemes. IP traceback identifies the source(s) of DoS or DDoS attacks, even in the presence of IP spoofing. Ideally, a good traceback system should have the following three features: (1) Ability to Handle Major DDoS Attacks (2) Scalability (3) Speed of Traceback After Attack. Existing traceback schemes need to be considered in order to get the background information needed to propose our new approach.

We analyze different existing schemes and extract advantages from each one. Our contribution begins with integrating a current solution to an equally complex problem. Two notable properties from quantum physics have been exploited to completely answer the problems associated with traditional cryptography. The same methods used to answer eavesdropping with quantum cryptography can answer IP Traceback. By combining quantum cryptography principles with proposed traceback schemes, it was found that new traceback will not be a problem. Even with the hardware devices in the current network infrastructure, only a small part of quantum principles helps us achieve a more efficient and accurate solution for IP traceback. Attacks will not be a problem in the quantum world.

Right now we are not in the quantum world. However, given the future network structure, an advanced scheme for traceback is proposed.

The remainder of the research project is organized as follows: In Section 2, we present the background objective of IP traceback. Section 3 presents related work for several IP traceback schemes as well as metrics measurements for each one. In Section 4, we present the fundamental knowledge of quantum mechanics and quantum cryptography. In section 5, an experimental quantum network is presented and discussed. In Section 6, we propose two main solutions: the quantum private channel and a new scheme called quantum network overlay. The conclusion is presented in Section 7.

II. Background

As the Internet becomes increasingly important as a business infrastructure, the number of attacks on it, especially denial-of-service attacks—TCP SYN flooding, Teardrop, Land—continues to grow. The lack of secure schemes that could be widely used has made it so imposters cannot be found or can easily escape. To the offender, the less risk there is of being exposed means the more likely they are to execute their crime. Furthermore, anyone attacked on the Internet knows the feeling of being helpless and not knowing what to do. Most individuals, including computer literate users, find it difficult to access emergency help and report Internet crimes. Even if they could, the party handling the case would require the legally obtained identification information of the criminal to secure as critical evidence in carrying out the investigation [1], [2].

IP traceback provides this critical evidence. To combat Internet crimes, there are several existing IP traceback schemes but most of them have their own advantages and disadvantages. One good method providing IP traceback is the architecture in which routers log data about packets and adjacent forwarding nodes, enabling us to trace IP packets to their sources even when the source IP address is forged [3]. Although designing a perfect IP traceback architecture is impossible, improving the current models is still the main objective for most experts who are working so hard to fight these crimes. The rising threat of cyber attacks, especially Distributed Denial-of-Service (DDoS), makes the IP traceback problem very relevant to today's Internet security.

III. Related Work

Having learned the state-of-the-art [5]–[11] and history [12] of the existing networks including the Overlay Network scheme can be considered as a starting point and further qualifies us to give reasonable solutions to the original problem in a different network environment. The following paragraphs summarize four preferred schemes along with their advantages and disadvantages.

A. Host-based traceback

The Host-Based traceback consists of three components, Traceback Coordination Center (TCC), robot (bot), and victim. The process begins when the attack on the victim is detected, starting with a notification from the victim sending their IP address to the TCC responsible for making the victim list. The bot downloads the victim list to inspect whether it has access to the victim or not. If it does, it sends the access records to the TCC. The TCC extracts the active IP address considered to be a Control and Command (C&C) server.

Although the Host-Based traceback scheme operates on the PC, all packets going out or in to the PC have to be recorded. The TCC then creates a victim list. The list is used to determine whether or not the PC is a zombie. It then processes the access records the PC sent to find the C&C servers. Configuration of the PC and TCC does not affect the configuration of other devices, a desirable quality for scalability. Security services are not specified between the PC and TCC. There is possibility for, modification, eavesdropping messages on the network, and IP spoofing violating integrity, confidentiality, and authentication respectively. These problems can be eliminated by applying existing security protocols to the scheme. Credible traceback depends on whether the victim's IP address and access records are secure between PC and TCC. The process to find traceback starts after Intrusion Detection System (IDS) (or Anti-Virus) at the victim, where attack packets are detected. This is the reason why traceback after attack is high.

Advantages:
- Dedicated to defending DDoS attacks
- Runs on the PC

Disadvantages:
- Only traceback to C&C Server, and not IP
- IDS detects an attack packet, which is a big assumption
- Large memory requirement
- Authentication not guaranteed between TCC and PC
- Infected PC reports access record for 10 minutes

The PC access record may cause a privacy issue, because all packets have to be recorded and reported.

B. Non-Intrusive IP Traceback

The Non-Intrusive IP traceback scheme uses sampled traffic under non-attack conditions to build and maintain caches of the valid source addresses transiting network routers. This approach is dedicated to DDoS attacks and even deals with IP Spoofing issues. The traceback is controlled by the White List (WL) and cached on the router. This scheme is non-intrusive, meaning it is not necessary to make any changes to the routers assisting in the traceback process. Built-in traffic sampling/monitoring and exporting tools in routers could be used to sample and report the required information to the WL caching devices during a learning process. Even if such tools are not built into the routers, we can make use of monitoring devices by installing them along the network paths instead. After an attack has been detected, the WL caching devices search for mismatches between the sampled traffic and cached data. All anomalies are sent back to the Traceback Manager to generate the attack graphs. Hence, it only requires one attack packet for traceback. The devices involved in traceback are properly managed and protected, but there is still a probability that the attacker could take over a device. The traceback can start right after detecting attack packets. However, there are still several unanswered questions, such as how to determine strategic points for internal zombie attacks and when to suspend the learning process in order to prevent records of the attack traffic flow being included in the WL.

Advantages:
- Non-intrusive
- Simple, fast and efficient with high coverage
- Low false positive rate

Non-intrusive, meaning there is no need to modify existing routers, victim or Internet protocols. The increase in speed is due to the simple computation for attack graph construction. The high coverage is due to the distribution of processing workload.

Disadvantages:
- Relies on a key assumption – routing scalability
- Needs a mechanism to detect DDoS attacks
- Only detects the closest point to the attack source

C. Distributed-Log-based IP Traceback

The Distributed-log-based (DLS) scheme for traceback considers Hierarchical IP Traceback System (HITS) and significantly combats some of its weaknesses. Three significant ideas contributing to traceback are the logging of packet marks right before they are replaced by new marks to improve marking utilization. Second, the Marking Agents (MAs) are carefully situated only on edge routers to take advantage of the extra resources. Finally, credible third party TSPs authenticate access to their records to protect against attacks.

The Traceback Service Provider (TSP) servers are managed and deployed by ISPs. Additional routers can easily be added between the TSP and MAs. The scheme is only an instance of PPM and an enabler of DDoS detection and therefore suffers the same consequences. TSP requests for traceback must be authenticated. Again, TSP is an instance of PPM and merely enables DDoS detection. The TSP is a credible third party. The scheme uses a logging technique.

Advantages:
- ISP incentive to provide chargeable security service
- MAs on edge routers, ISPs exploiting extra resources
- If security evaded, TSP knows the identity

- Less packet information to carry-out DDoS traceback
- Packet information stored before overwritten

The information is stored for an infinite amount of time and is not overwritten as in PPM.

Disadvantages:
- ISP invests initial amount of money to implement TSP
- Edge routers may not be fixed
- ISP implements security authentication mechanism
- Enables detection, but does not defend DDoS attacks
- Still an instance of PPM, not marking every single packet

The edge router of today may not be the one of tomorrow. Marking every single packet would be ideal.

D. Stateless Single-Packet IP Traceback

Stateless Single-Packet IP traceback scheme is based on a packet marking technique. The packet marking procedure is simple. The basic concept is that every router (upstream router) on the attack path marks its IP address in a packet and a victim performs reconstructing the path as a starting point. In other words, before forwarding a packet, each router on the attack path inserts its own IP address into the Bloom Filter of the packet. After the all related routers complete the marking and the victim receives the attack packet, the victim initiates a path reconstruction procedure to identify the source. The process is as follows: The victim inspects all neighbors in the Bloom Filter of the received attack packet. The next router recognized by the filter is considered as the upstream router. This upstream router receives the respective Bloom Filter from the victim and checks the next upstream router recognized by the filter. This procedure is iteratively repeated on each router to reconstruct the actual path until no neighbor router is recognized.

In the scheme, the complete route of each packet can be individually determined, which is scalable. In addition, no information is stored in the network infrastructure such as a router. It also not only avoids the appending processing overhead and packet fragmentation, but also introduces very low additional overhead to the forwarding procedure. Any help from network operators are not involved in the scheme because of automated reconstruction procedure and independent of manual intervention. However, all routers are involved to get accurate path in the scheme, and identifying the attacker is out of the scope. Furthermore, false negatives are introduced due to the Bloom Filter. [13]

Advantages:
- Individually determined path, which means scalable
- No information at all is stored in the network infrastructure
- Avoid processing overhead and packet fragmentation
- Low additional overhead to the forwarding procedure
- Automated reconstruction

Disadvantages:
- All routers are involved
- Attacker is not identified, only routers
- False negatives are introduced

Table 1 summarizes the above reviews.

TABLE I
COMPARISON OF MODERN TRACEBACK SCHEMES

Name of Traceback Scheme	Host-Based	Non-Intrusive	Distributed-Log-based	Stateless Single-Packet
ISP Involvement	None	Low	Fair	Low
Scalability	High	High	High	High
Number of Attack Packets Required	Many	1	Many	1
Ease of Evasion/ Protection	Low	Fair	High	Low
Ability to Handle Major DDoS Attacks	Good	Good	Low	Good
Credible Traceback	Fair	High	High	High
Traceback After Attack	High	High	Fair	High

IV. QUANTUM

The initial idea that sparked the evolution movement was the quantum cryptography chapters in literature. Two notable properties from quantum physics have been exploited to completely answer the problems associated with traditional cryptography. It can be inferred that the same methods used for quantum cryptography can be adapted to quantum IP Traceback. This is an area where this contribution would have more prestige. The same measurement table used above will continue to be used as the metric to measure the new IP Traceback scheme.

On the way to proposing a new algorithm for IP traceback, we first need to illustrate the very basics of quantum physics. The following paragraphs summarize the primary reference [14] used to solidify the understanding of quantum computing with an example in quantum cryptography. The book, although not exactly straightforward, was the most basic introduction to quantum computing found from all the researched literature.

A. Fundamentals

According to Moore's law, the amount of information able to fit on a transistor (number of transistors able to fit onto an integrated circuit) doubles every 1.5 years. Assuming the law holds true, it means in less than roughly a few decades the components of the future PC will become so tiny to actually come down to the atomic level. If the existing system of bits is not supplanted by a new smallest unit of information, errors will be introduced into the computing. At the atomic level, the

particles, behave differently, then the larger components of today, and therefore we no longer will be able to rely on traditional bits. The fundamental difference between the current information age and the quantum age is in the power used to communicate. Currently messages are sent with electricity; in the future messages will be sent with light. The light can be sent over cable wires, fiber optic wires, or free space. All communication will be sent as light signals.

The notation for binary values 0 and 1 in the quantum world are $|0\rangle$ and $|1\rangle$ respectively [15]. Currently, the smallest unit of information is the bit (binary digit). In the future, the smallest unit of information will be the qubit (quantum bit). In the binary information age, the physical component of communication is achieved by sending electricity signals over copper wires represented as binary data for people. In contrast in the quantum information age, the preferred physical component of communication is achieved by sending light signals over fiber optic wires represented as four states instead of the traditional two states. The symbols + and $\times$ represent the four states. One state by the vertical line, one by the horizontal line, both superimposed into the plus symbol and one for each diagonal both superimposed into the "times" symbol.

After gaining a solid understanding of the fundamentals, the story behind quantum cryptography, and the architecture of a quantum network, the researchers set out to find more quantum physics phenomena to exploit. First consider, the information transmitted through quantum private channels is traveled through a newly developed technology – fiber optics.

B. Fiber Optics

The optical fiber is a glass fiber that carries light along its length instead of electrical signal. They are widely used in fiber-optic communications for providing transmission over longer distances and at higher bandwidths than current technology. Signals traveling along the fibers have such advantages as less loss, immured to electromagnetic interference, and the signals do not electromagnetically radiate. The fibers are immune to electromagnetic noise from both optical and electrical interference. Because of the advantages over electrical wires, optical fibers have begun to largely replace copper wire communications in many networks.

An optical fiber is a cylindrical dielectric waveguide and consists of a core surrounded by a cladding layer, both of which are made of dielectric materials (see Fig. 1). The fiber transmits light by the process of total internal reflection meaning that when light traveling in a dense medium hits a boundary at a steep angle, it will be completely reflected.

Two types of fibers are generally used. Multi-mode fibers support many propagation paths or transverse modes. They have a larger core diameter and may be analyzed by geometrical optics. The multi-model fibers are usually used for short-distance communication links and for applications where high power must be transmitted. Single-mode fibers are designed to only support a single ray of light. They are often used in high-precision research purposes, because the allowance of only one propagation mode makes the light easier to focus properly. Like multi-mode optical fibers, single-mode fibers also exhibit modal dispersion resulting from multiple spatial modes but with narrower modal dispersion. Single mode fibers are therefore better at retaining the fidelity of each light pulse over longer distances than multi-mode fibers. Hence, single-mode fibers can have a higher bandwidth than multi-mode fibers. However, multi-mode fiber is better than single-mode optical fiber at light colleting because of the larger core size. But the limit on speed times distance is lower. [16]

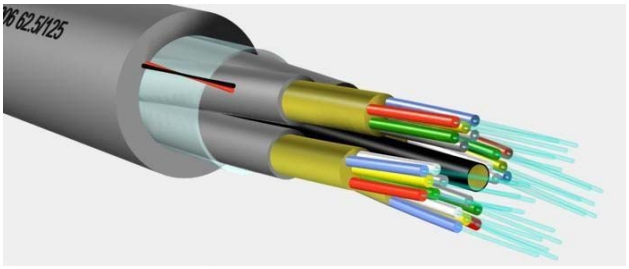

Fig. 1: *A fiber optical cable.*

Optical fibers are stored in optical fiber cables. Like Fig. 1 shows, the cable is coated individually with plastic layers and contained in a protective tube suitable for the environment. Fiber cables are connected to each other by splicing, i.e.) joining two fibers together to form a continuous optical waveguide. From a physical aspect, joining lengths of optical fiber is a more complex procedure than joining electrical cable because of the need for stripping, careful cleaning, precision cleaving and other specialized operations. At the end of the procedure, these fiber cables are connected with terminal equipments, which convert signals between electrical and light.

With little attenuation of light propagation and higher bandwidths, fiber optic is especially advantageous for long-distance communications and high-demand applications. Additionally, each fiber can carry many independent channels, each using a different wavelength of light. The current laboratory fiber optic data rate record is multiplexing 155 channels, each carrying 100 Gbps over a 7000 km fiber by Bell Labs in Villarceaux, France [17].

Shown as follows, fiber optics provides several important features to keep the communication fast and secure.

- Low error rate and low signal loss
- High security: Extremely difficult for intruder to tap
- High capacity bandwidth: Fast point to point transmission
- High resistance: Safe near high-voltage equipment
- Low weight and volume: Various suitable environments

C. Quantum Cryptography Patterns

The "secret" key(s) used to decrypt and encrypt messages in traditional cryptography are not guaranteed to be secret at all. A quantum computer can easily find the keys. The answer to this problem is to exploit two of the physical properties of quantum physics: The Heisenberg Uncertainty Principle and the polarization in light photons (Polarization Principle). These quantum properties are exploitable in the key generation and key distribution steps found in traditional cryptography called quantum key distribution (QKD).

A set of traditional bits are randomly chosen and converted into polarized light photons before they are sent over a quantum

channel. These bits will eventually be used to generate a secret key to establish secure communication. To verify the bits were not intercepted by an eavesdropper, a subset of bit positions, and corresponding bit values are sent over the classical channel to the intended receiver (see Fig. 2).

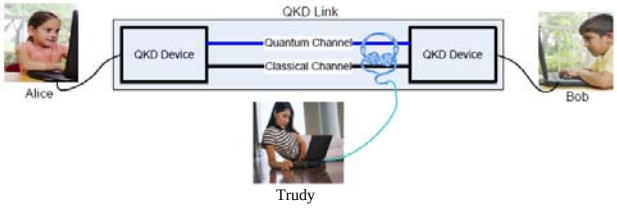

Fig. 2: Romain Alléaume, "Quantum Key Distribution and Cryptography" (2007), (http://arxiv.org/PS_cache/quant-ph/pdf/0701/0701168v1.pdf)

At about the same time, the corresponding polarizer orientations are sent through the quantum channel to the same receiver. The receiver sends the corresponding calcite crystal orientations for the same bit positions they have back to the sender. If the orientations are the same on both sides and the bit values in those positions are the same, the key can be generated using the subset of bit positions and their values. However, if the positions having the same orientations have different bit values at those positions, it means an eavesdropper has intercepted the message. The error is immediately noticeable by the channel, it is shut down, and the message is rerouted to a different channel.

Two examples are used to further illustrate how quantum cryptography distributes secret keys from the risk of eavesdropping. Table II is a simple example to show how the key is delivered from Alice to Bob with no eavesdropping detected. Directly following the table is the specified definitions of polarization symbols to values.

TABLE II
SHARED KEY GENERATED, NO EAVESDROPPING DETECTED

Alice sends bits	1	1	1	1	1	0	0	1	0
Alice randomly chooses polarizer positions	×	+	×	×	×	×	×	×	×
Photon Alice sends	\	-	\	\	\	/	/	-	/
Bob randomly chooses polarizer positions	+	+	×	+	×	×	+	×	+
Bob reconstructs bits	0	1	1	1	1	0	0	0	1
Alice sends subset of positions		+	×			×			
Bob sends his corresponding positions		+	×			×			
Shared secret key generated		1	1			0			

Superimposed as +:

1) Horizontal (-) = 1
2) Vertical (|) = 0

Superimposed as x:

3) Diagonal (/) = 0
4) Opposite diagonal (\) = 1

Table III below shows a detected error. The intruder (Trudy) attempts to intercept the information which should only be accessible to Alice and Bob. See the highlighted 1 and 0 in the table. The value bit that Bob reconstructs is not the same as the original bit Alice sent. The mismatch in bits identifies the intruder has changed the message by observing it.

TABLE III
NO SHARED KEY GENERATED, EAVESDROPPING DETECTED

Alice sends bits	1	1	1	1	1	0	0	1
Alice randomly chooses polarizer positions	×	+	×	×	×	×	×	+
Photons Alice sends	\	-	\	\	\	/	/	-
Trudy randomly chooses polarizer positions	+	+	×	+	×	+	+	×
Trudy reconstructs bits	0	1	1	1	1	0	0	1
Trudy uses same polarization positions	+	+	×	+	×	+	+	×
Photons Trudy sends	|	-	\	-	\	|	|	\
Bob randomly chooses polarizer positions	+	+	×	+	×	×	+	×
Bob reconstructs bits	0	1	1	1	1	1	0	1
Alice sends subset of positions		+	×			×		
Bob sends his corresponding positions		+	×			×		
Error detected		1	1			0		

V. EXPERIMENTAL QUANTUM NETWORK

A. Small Quantum Network

Quantum IP trackback aims at providing IP trackback technology that relies on the properties of quantum mechanics. So far, there is no such analysis for quantum IP trackback. No previous research direction could lead us towards further research. All ideas are virtually brand new, either two ideas can be combined together, or a totally new method invented. Moreover, lack of any physical quantum network environment also makes it a major problem for practical research (theorist versus experimentalist dilemma). To overcome this challenge, an attempt was made at setting up a very small quantum network. The basis of the network can be seen in Fig. 3 [24].

The experiment is by no means complete. The purpose of this section is to give future work the initial place to begin building a small quantum network for experimentation. The small network will give the environment needed to experiment with ideas, test methods, and form experimental data. The purpose of the experiment is to help build practical evidence, including experimental data, to support hypotheses.

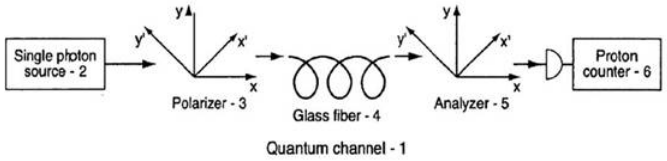

Fig. 3: *Base of small quantum network.*

The experiment is by no means complete. The purpose of this section is to give future work the initial place to begin building a small quantum network for experimentation. The small network will give the environment needed to experiment with ideas, test methods, and form experimental data. The purpose of the experiment is to help build practical evidence, including experimental data, to support hypotheses.

Taken from [14] the LED light should be on the green frequency. On the receiving side of the communication sits an analyzer and photon detector. The analyzer is made of two, calcium carbonate $CaCO_3$ (calcite) crystals, oriented in opposite directions on the Cartesian plane X-coordinate. The light signals are decoded over the fiber optic cable by toggling the two calcite crystals up and down decomposing the message signal from the sender.

Light emitted from the LED lights used have no direction, meaning the light is spread in all directions, similar to how lights in the ceiling of a room bursts in all directions, the light particles spread in all directions [15].

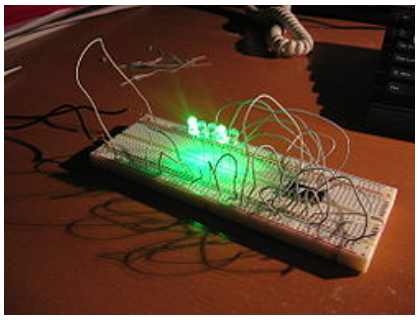

Fig. 4: *Circuit board with green frequency LED.*

The following is the list of parts needed to start building the network.

Green frequency LED light(s) (Description: LED green clear round, Part Number: P302, Manufacture Number: LN31GCPHL, Origin: Japan)
Breadboard (circuit board), (see Fig 3.[1])
Collimator, or convex and concave lenses (or two possibly modified magnifying glasses), (see Fig. 4)
Positive (red) and negative (black) wires
Two AA batteries (giving power to the breadboard)
Calcite crystals (at least two), or Photo Detector (or significantly less expensive Photo Transistor) [18], [19]
Polarizer

[1] The idea originated from [15] in the diagram.

These particular LED lights are 1.7 – 2.4 volts. The DC power supply required to power the circuit board can therefore be 2.0 volts (or two 1.5 volt AA batteries).

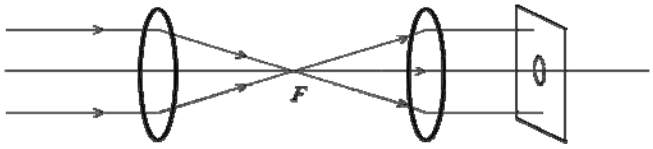

Fig. 4: *Focus light with no direction.*

When first experimenting, one should make certain the voltages are compatible with the equipment (e.g., pay particular attention to wavelength selection, it must be matched with your LED.) before actually running the experiment. Plug the red and black exposed ends of the wires into positive and negative slots on the circuit board. Place the batteries standing on top of each other, positive end connected to negative end. Place the exposed wires on the ends of the combined battery to provide the power to the circuit board, giving light to the LED bulb.

The quantum network could also be built with a multiplexer (digital switch) sitting between connection points. Then the battery does not control turning on the current, the switch can be turned on and off and the ends could additionally be connected to other private channels or if using free space instead of fiber optic cables, face the communication beam leading to other nodes to simulate private channels.

VI. Solutions

A. Quantum Private Channel

Current existing traceback schemes are becoming strong enough to defend many of the network attacks, even DDoS attacks. The only real concern is telnet spoofing, but this can be combated with authentication. For example, “What if the organization wants such privileged users to authenticate themselves first before being allowed to create Telnet sessions to the outside world.” [20] For another example, consider current ISPs already offer IP traceback service indicating when someone attacks you from, for instance say, Japan, then so what if someone is probing your system, the situation becomes, there is nothing anyone can do about it. In our solution, the problem remains the same; however, the network domain has changed from the traditional network to the quantum network. We strongly believe that there is a perfect solution for IP traceback in quantum-based network environment. This is an area where our contribution would have more of an impact. Fig. 5 shows how our scheme fits into the existing architecture of existing proposed traceback schemes.

Two notable properties from quantum physics have been exploited to completely answer the problems associated with traditional cryptography. It can be inferred that the same methods used for quantum cryptography can be adapted to quantum IP Traceback. The endless search for exploitable quantum phenomen including the Heisenberg Uncertainty Principle, Polarization Principle, and others not considered, such as the non-cloning theorem, superposition, teleportation,

interference, and entanglement, which can be used for IP Traceback. All the research work done concerning quantum phenomena were found to be unnecessary for our solution, or not to be as directly useful as was hoped. After much effort was put forth into researching the different quantum phenomena, looking for exploitable properties, a very simple solution to the problem of IP Traceback and spoofing source addresses was discovered. The idea was realized by digging in the trenches of quantum, so to speak, and earning the ability to appreciate the answer there in plain view all along.

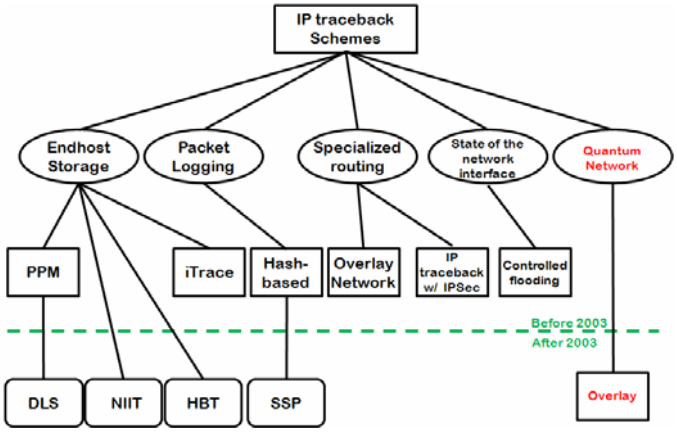

Fig 5: *Existing and newly proposed traceback schemes.*

The whole objective of the quantum is if one measures something he (she) upsets that something. During our research, it was noticed by moving the current network of today—the Internet, into a quantum network, it would no longer be a public Internet of shared lines at all. Every transmission of data could be done over private fiber optic cables, where the fibers in the cable are all private channels. Each connected device has a unique frequency of light used for communication signals [21]. The channels are separate light signals over the same fibers. Considering the physical aspects of wires, an attack on copper wire through tapping can easily be achieved by wrapping another copper wire around the copper connection to eavesdrop communications [22]. The fiber optic channels lying on the ocean floor would take a submarine to accomplish splicing. Fiber splicing the line is the only way to eavesdrop and is by no means an easy task and must be accomplished by a specialized professional.

Our contribution is called Quantum Private Channels (QPC). The idea is in recognizing the eventual certainty of Moore's law reaching a frightening threshold, the realization the way modern computation is required to change once our world moves to the atomic level and the confidence there is in the migration to quantum. Having retrospect before designing the quantum network on its side, commercial quantum networks can be designed with private quantum channels (our idea) where spoofing is not possible. It is critical to notice there is no longer the need for IP packet headers and other structured information contained within the packet. Sometimes, new technology "advances" actually hinder the overall experience of the technology. With retrospect in mind, we propose quantum private channels are used with fiber optic cable as the medium. In essence, the idea proposed requires us to go back in time, and revive the old telephony system using "point-to-point transmission technology" [23]. In place of broadcasting messages through every computer on the Internet between the source and destination, we propose going back to point-to-point connections, connected over long distances with switches. When the communication is initiated, the automated operator at the switch plugs the wire into its requested end point. This is the main problem with existing networks. We propose to re-consider the benefit analysis of the telephony system, considering its drawbacks and benefits. Secure communications, information assurance, and dedicated bandwidth provided by quantum private channels together outweigh costly connections.

In this scheme DDoS attacks are not possible if one does not allow the attacker access to the line. Otherwise, if allowed access, the attacker can launch an attack. The solution to this problem is the identity of the attacker is known. Both sides already know the exact identity of the other side of the communication. There is no longer the need for IP packet headers and other structured information contained within the packet. The Web site server knows exactly what client it is communicating with and the opposite is likewise true.

B. Quantum Network Overlay

The Quantum Network Overlay (QNOL) is based on the existing overlay network scheme. In the existing overlay network, a tracking router (TR) is introduced and lies in the middle of the network, where it can monitor all traffic. In order to accomplish the goal, a generic route encapsulation tunnel is built from each edge router to the TR. Once the appropriate configuration from edge routers to TR is made, all traffic from the source edge router would be forced to travel though the tunnel to the TR, and then from the TR to the destination edge router. Logically, it is only one hop from an edge router to the TR. However, in reality, many tracking routers will be used for this scheme because of the heavy load of data transmission. The TR utilizes signature-based intrusion detection. When an attack is detected, the attack packet will constitute an intrusive action. Hence, the origin of the attack can be identified because it is only one hop away.

The existing network overlay is a good idea, but has severe limitations causing it not to score well on standard metrics. One major problem is that the TR acts as a center of the whole network, where the huge workload could affect transmission speed and efficiency.

Therefore, fundamental differences in the scheme are needed. The new proposed scheme uses optical fibers to transmit qubits in preference to regular wires for the generic route encapsulation tunnel, and then the large quantum switch in preference to the large TR (tracking router), (see Fig. 6). The signature-based intrusion detection will still be utilized by the quantum switch for attack packet detection. Although, the changes from the existing to the new scheme appear to be trivial, looking at it closer reveals that the new scheme makes a

huge impact on security. To send a packet, the sender transmits binary messages on the existing network. The binary messages are converted into a sequence of qubits through a polarizer stored in the source edge router. Then, the qubits are transmitted on the quantum private channels through the quantum switch to the destination edge router. After the destination edge router decodes the sequence of qubits into binary, by the analyzer, which is also stored inside the quantum router, it sends the binary message to the receiver. Once an attack packet is detected the attacker's source edge router could be identified immediately.

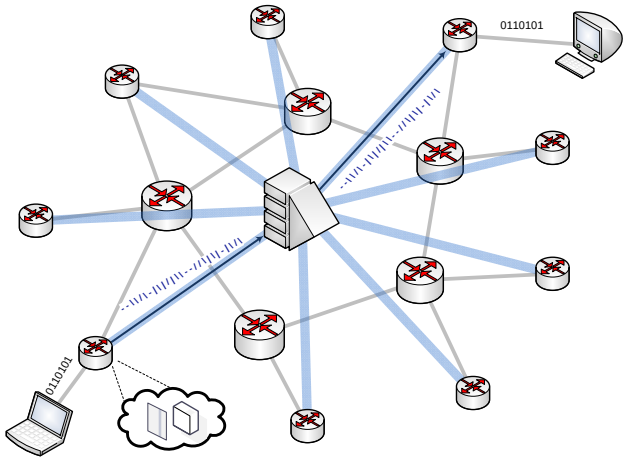

Fig. 6: *Quantum Network Overlay*.

It is however, not enough to only identifier the attacker's edge router. In order to further track the attacker behind this edge router, 100% of the packets will be marked inside the network. As seen in Fig. 7, when a packet transmitted from a user to the external Internet, it will pass several internal switches and routers. When the packet first arrives at the switch, the switch will mark its own IP address (100.110.0.1) into the packet's header and sends it to next router. The next router will also mark the IP address of 100.110.0.2. When this packet reaches the edge router, a path for the transmission is formed inside the header, which looks like 100.110.0.1, 100.110.0.2, 100.110.0.3, 100.110.0.4 as the example shows. Since the packets from different end users would have different travel paths, the attacker could be detected even if he/she spoofs the source IP address.

This approach greatly improves the performance of communication because the quantum router processes more qubits in less time, based on quantum principles. Additionally, using fiber optics for generic route encapsulation tunnel provides a higher bandwidth and faster speed, compared with the current overlay network, which a single TR is unable to handle the load of packets from the whole network. This quantum network overlay scheme also provides the solution for tracking the real attacker by marking path routers' IP addresses in each packet's header. Since only routers for the network behind the edge router are marked, the space of a packet's header for storage is no longer a concern. However, ISP involvement in this scheme is large because the ISP has to perform a traceback as well as identify the attack completely on its own. Additionally, equipment, such as quantum switches and IDS servers would have to be purchased by the ISP.

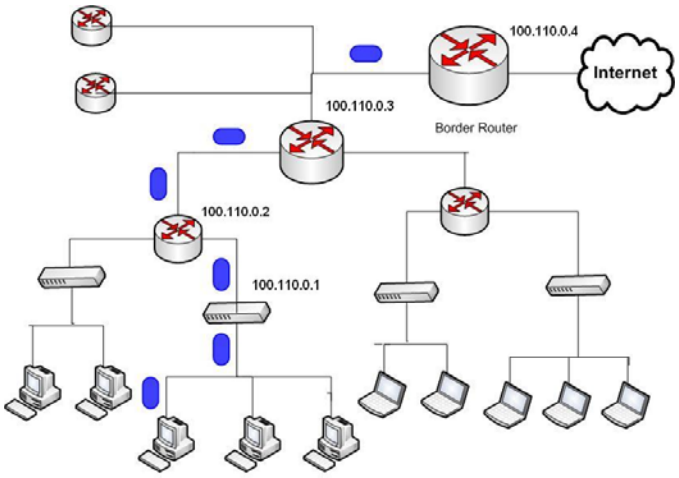

Fig. 7 *Marking path for each packet in the network.*

The statement made earlier at the beginning, specifying a good traceback system should have the following three features: (1) Ability to Handle Major DDoS Attacks (2) Scalability (3) Speed of Traceback After Attack, is satisfied by QNOL.The system scores well in all three categories, and additionally satisfies the modern standard metrics used for current evaluation of proposed schemes, thereby satisfying the original objectives.

VII. Conclusions

The basic goal of this work was to propose a new scheme for IP traceback based on future networks. Existing traceback schemes were considered before approaching a new proposed method. Several existing proposed schemes are becoming strong enough to nearly defend the problems and risks associated with network attacks requiring IP traceback. Two notable properties from quantum physics have been exploited to completely answer the problems associated with traditional cryptography. It was inferred, the same methods used for quantum cryptography can be adapted to quantum IP Traceback. Future quantum networks are an area where our contributions would have more prestige than trying to contribute small and hard fought for improvements over existing proposed schemes. The whole idea behind the quantum is if one observes something he (she) disturbs that something. It was noticed during the research, and studied in later stages, the problems associated with IP traceback are eliminated by moving the modern network environment to quantum networks with private channels over fiber optic cables. Each private communication line knows exactly where the messages came from and ends at with this architecture.

TABLE IV
MEASUREMENT FOR QUANTUM NETWORK OVERLAY

Name of Traceback Scheme	Quantum Network Overlay
ISP Involvement	High
Scalability	Fair
Number of Attack Packets Required	One
Ease of Evasion / Protection	Low
Ability to Handle Major DDoS Attacks	Good
Credible Traceback	High
Traceback After Attack	High

Our contribution declares future networks should be designed on point-to-point transmission technology to eliminate the requirement of IP traceback based on security risks, threats and attacks. The idea is developed further by borrowing aspects from the proposed overlay network scheme and laying the quantum private channels and switches over the existing network infrastructure.

ACKNOWLEDGMENT

The authors would like to thank Zheng Huang for her elegant explanation of quantum physics, Greg L. Vitko for his ideas related to quantum communication, and Dr. George Balster Martins, Associate Professor of Physics, for outside of department support. Extra thanks goes to Jiachun Xie for explaining the physical side of fiber optic cables, Yue Xiang and Mohammed Ibrahim Ayub Khan for providing electrical information, and Ruchir Sharma for adding the idea about the switch to the small quantum network. The authors would also like to thank Kelly Coe, George Cafcalas, Benjamin Malburg, Ashley Treadwell, Allison Crosley, and Philip Porter from the Oakland Writing Center, for editing and proofreading their documents.

REFERENCES

[1] S. C. Lee and C. Shields, "Tracing the source of network attack: A technical, legal and societal problem," in *Proceedings of the 2001 IEEE Workshop of Information Assurance and Security*, 2001.

[2] R. Pang, M. Allman, V. Paxson and J. Lee, (2006, January). The devil and packet trace anonymization. *ACM SIGCOMM COMPUTER COMMUNICATION REVIEW*, 36(1), pp. 29-38.

[3] T. Baba and S. Matsuda, (2002, March). Tracing network attacks to their sources. *IEEE Internet Computing*. 6(2), pp. 20-26.

[4] S. Alcock, D. Lawson and R. Nelson, "Extracting application objects from TCP packet traces," in *Proc. Telecommunication Networks and Applications Conference, ATNAC*, Australia, 2007, pp. 151-156.

[5] Y. Jing, J. Li, X. Wang, X. Xiao and G Zhang, (2006, April). A Distributed-Log-based IP Traceback Scheme to Defeat DDoS Attacks. *Advanced Information Networking and Applications, AINA06.* 2, pp. 25-32.

[6] M. Sung, J. J. Xu, J. Li and L. Li, (2008, December). Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation. *IEEE/ACM TRANSACTIONS ON NET-WORKING (TON)*, 16(6), pp. 1253-1266.

[7] L. Lu, M. C. Chan and E. Chang, "A general model of probabilistic packet marking for IP traceback," in Proceedings of the 2008 ACM symposium on Information, computer and communications security, 2008, pp. 179-188.

[8] Y. Jing, X. Wang, X. Xiao and G. Zhang, "A Logless Fast IP Traceback Scheme Against DDoS Attacks in Wireless Ad-hoc Network," in *IET International Conference on Wireless Mobile and Multimedia Networks Proceedings (ICWMMN)*, 2006, pp. 414-418.

[9] K. TAKEMORI, M. FUJINAGA, T. SAYAMA and M. NISHIGAKI, "Host-based traceback; Tracking bot and c&c server," in *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communicatio*n, ICUIMC, 2009, pp. 400-405.

[10] V. L. L. Thing, M. Sloman and N. Dulay, "Non-Intrusive IP Traceback for DDOS Attacks," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security, ASIACCS*, 2007, pp. 371-373.

[11] F. Zarai, S. Rekhis, N. Bourdriga and K. Zidane, "SDPPM: An IP Traceback Scheme for MANET," in *12th IEEE International Conference on Electronics, Circuits and Systems*, 2005, pp. 1-4.

[12] A. Belenky and N. Ansari, (2003, July). On IP Traceback. *IEEE Communications Magazine*. 41(7), pp. 142-153.

[13] R. P. Laufer et al., "Towards Stateless Single-Packet IP Traceback," in *Proc. The 32nd IEEE Conference on Local Computer Networks (LCN)*, Dublin, 2007.

[14] W. Clearwater, *Ultimate Zero and One, Computing at the Quantum Frontier*, New York, NY: Copernicus, 2000, pp 143-156.

[15] Z. Huang, Oakland University Physics Lab., Rochester, MI, private communication, October 2009.

[16] N. Thorsen, *Fiber Optics and the Telecommunications Explosion*, Upper Saddle River, NJ: Prentice Hall, 1998, pp 7-25.

[17] S. Higginbotham. (2009, Sep. 28). Alcatel Boosts Fiber Speed to 100 Petabits in Lab [Online]. Available: http://gigaom.com/2009/09/28

[18] I. E. Kreslo, (2009, Deccember). Photon Detectors [Online]. Available: http://www.lhep.unibe.ch/img/lectureslides/57_2009-10-12_PhotonDetectors-I.pdf

[19] Digi-Key Corporation, (2009, December). Photo Transistors [Online]. Available: http://search.digikey.com/scripts/DkSearch/dksus.dll?Cat=1967049&k=photo%20transistor

[20] H. Fu, CSE 681 Information Security, Firewall Slides, Oakland University, Rochester, MI, Firewall Slides, 2009.

[21] J. Xie, Oakland University Kresge Library, Rochester, MI, private communication, November 2009.

[22] G. L. Vitko, Telephone Interview., Rochester, MI, private communication, November 2009.

[23] A. S. Tanenbaum, *Computer Networks*, Upper Saddle River, NJ: Prentice-Hall, 1996, pp 7-8.

[24] W. Dultz, H. Schmitzer, L. Beresnev and E. Hildebrandt, "Quantum Cryptography System for a Secure Transmission of Random Keys Using a Polarization Setting Method," U.S. Patent 6 748 081, July 20, 1999.

About equal effort was put forth by each team member. Sangsig Kim, read, summarized, and wrote in the Final Report the subsections of the two papers, "Towards Stateless Single-Packet IP Traceback" and "Host-based traceback; Tracking bot and c&c server". He improved upon the idea and wrote part of the Quantum Network Overlay section. He also made all the presentation slides and animations.

James G. Schiiller read, summarized, and wrote in the Final Report the subsection of the paper entitled "A Distributed-Log-based IP Traceback Scheme to Defeat DDoS Attacks". He was responsible for writing the Final Report. He additionally did most of the work on the small quantum network. Mr. Schiiller proposed the idea of the private channel.

Qianhua Gao read, summarized, and wrote in the Final Report the subsection of the paper entitled "Non-Intrusive IP Traceback for DDOS Attacks". She researched and wrote the entire fiber optics section. She drew nearly all of the diagrams. In addition, she developed and maintained the entire Web site. Furthermore, she invented and wrote the quantum network overlay section.