Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 7, July 2017, pg.220 – 226

Hyper Speed Signalling: The Next Step To Prevent Cyber Attacks

Ms. Poonam M. Mahajan

Assistant Professor, Bhusawal Arts, Science and P. O. Nahata Commerce College, India

amritamah@gmail.com

Abstract— This paper focuses on hyper speed signalling paradigm, which enables network administrator to work with Flash-like superpowers. The hyper speed signalling relates to use of optimal (hyper speed) paths for command and control traffic and suboptimal (slower) paths for all other traffic in order to implement sophisticated network service differentiation and defensive techniques. A reaction time window is created to ensure that packets sent along hyper speed paths can arrive sufficiently in advance of malicious traffic in order to alert network devices and initiate defensive actions. The defense techniques enabled by hyper speed signalling include distributed filtering, teleporting packets, quarantining network devices, tagging and tracking suspicious packets, projecting holographic network topologies and transfiguring networks. The paper also discusses the principal challenges involved in implementing hyper speed signalling in MPLS networks.

Keywords— ATM, ISR, MPLS, Omnipresence, Precognition, VPN etc.

I. INTRODUCTION

In military mail services security is more precious factor. The ability to deploy Paul-Revere like sentinel messages could help to improve defensive postures. These sentinel messages could out run malicious traffic. This suspicious traffic can be slowed down slightly to enable sentinel messages to carry out their task. Travelling by speed more than light is not possible but the "Hyper Speed" can be created by slowing down all other paths. This paper highlights that Hyper Speed Signalling uses optimal paths (hyper speed) for higher priority traffic and suboptimal (slower) paths for other traffic.

Hyper speed signalling provides teleporting of packets, teleporting in which matter gets converted into minute particles or energy at one point and recreated in original form at another, quarantining network devices means isolating data transmissions to prevent viruses, worms or other malware attack. It gives tagging and tracking of suspicious packets that result in mitigation efforts. It also projects holographic topologies and transfigure networks. This paper describes the hyper speed signalling paradigm, including its core capabilities and implementation requirements for MPLS networks. Ranging from distributed filtering and teleportation to quarantining and network holography, are highlighted.

II. HYPER SPEED SIGNALLING

Hyper Speed Signalling uses optimal paths (hyper speed) for higher priority traffic and other is sent along suboptimal (slower) paths. In general one or more hyper speed paths may exist and multiple slower paths between two nodes are available. Distinction between optimal and suboptimal path is that different reaction windows available for a hyper speed path compared to slower paths. These different windows provide varying amount of time to accomplish defensive actions (depends upon nature of priority) e.g. suspicious data could be sent along slowest paths.

Hyper speed paths need not be reserved only for command and control traffic. Certain time-critical traffic, such as interactive voice and video communications, could also be sent along faster, and possibly, hyper speed paths. Consequently, a suboptimal path should incorporate the smallest delay necessary to obtain the desired reaction time window. Different reaction windows are available for a hyper speed path compared to different slower paths. These different windows provide varying amount of time to accomplish defensive actions (depends upon nature of priority) e.g. suspicious data could be sent along slowest paths.

III. CORE CAPABILITIES

Precognition is provided by hyper speed signalling. Precognition is nothing but advance warning about attack. This implements sophisticated network defense techniques. The advance warning provided by Hyper Speed Signalling enables a network to employ "precognition", and react to an attack before it reaches the target. Precognition strongly relates to defensive actions.

One of the capabilities provided by Hyper Speed Signalling is that network administrator can identify a threat, or target packet arrives at a node under attack. There are two ways for identifying threats, first is to track multiple target packets and correlate information about all target packets, regardless of their locations in the network. Second way uses multiple hyper speed ways, one for each target packet under observation.

Network administrator can send a hyper speed signal to any node in the network before target packet arrives, referred as "Omnipresence". Omnipresence with respect to multiple paths has two versions: Stronger, there is only one flash and this flash arrives before all packets under consideration arrive at their destination; Weaker, multiple flashes, one for each packet.

Another core capability is the opportunity to collect intelligence, conduct surveillance of the network, and inspect the network. These actions are referred as Intelligence, Surveillance, and Reconnaissance (ISR). Intelligence is high level planning in nature; it involves the integration of time-sensitive information from all sources into concise, accurate and objective reports related to the threat situation. Reconnaissance, which is tactical in nature, refers to an effort or a mission to acquire information about a target, possibly a one-time effort. Surveillance lies between intelligence and reconnaissance. It refers to the systematic observation of a targeted area or group, usually over an extended time. The scope and speed of ISR capabilities depends on connectivity of nodes in network via hyper speed paths and reaction time windows offered by paths.

Tagging provides identifying suspicious packets, projecting holographic network topologies and transfiguring network, which means reshaping a network, to adapt environment and context.

IV. MPLS

Circuit switching and packet switching are two paradigms of transporting traffic across network. Circuit switching provides low latency and high Quality of Service (QoS), e.g. frame relay, ATM. IP in OSI is packet switched. Service providers give network with flexibility of IP and speed of Circuit switching. Packet switching connects heterogeneous networks to enhance QoS and flexibility. In MPLS (Multi Protocol Label Switching) Overlay model is used. ATM switches are unknown to IP routing and IP routers are unknown to ATM infrastructure. ATM network presented in virtual topology and IP is used to route traffic across this network. IP routing control paradigm uses forwarding mechanism. IP network have hierarchical model because of Classless Inter Domain Routing (CIDR). IP addresses consist of network prefix followed by host id. IP node forwards packets according to the most specific, e.g. "longest match", route identified by destination address.

For MPLS, more general forwarding mechanism is used called "Label Switching". In MPLS connected oriented nodes are directly peered with connectionless technologies by transforming ATM switches to IP routers. ATM switches directly participate in IP routing protocols (RIP and OSPF) to construct label switched path (LSP). LSPs are implemented in ATM switches as virtual circuit that enables existing ATM technology to support MPLS forwarding mechanism. Within MPLS core, label switching depends on packet label to select

LSP. Any algorithm that constructs LSP and specify labels can be used to control MPLS network. Hyper Speed enables distributed filtering, teleporting packets, quarantining network devices, tagging and tracking suspicious packets, projecting holographic network topologies and transfiguring networks.

A. Label Switching

Connectionless IP routing is converted Connection oriented by overlaying Network layer function with Data Link layer function. Label Switching overcome the limitations that presents in the circuit Switching. IP address is converted into Labels according to the class and type of services like categories and priori-ties. An intermediate router uses only the labels for further routing of destined IP packets with appropriate label. This technique is used in MPLS. An MPLS frame uses various Data link frames like ATM, Frame Relay, and Ethernet. Since MPLS uses Label Switching and supports multiple protocols, it is called as Multi Protocol Label switching.

B. Label

A label in MPLS is used as the routing code like STD code in circuit switch. It identifies the path a packet should traverse in the MPLS domain. Label is encapsulated in a Data link layer. Thus new layer is formed in between Network layer and Data link layer in the OSI model. The name of the new layer is MPLS SHIM layer. The shim is composed of 32 bits out of which 20 bits are allocated to the label also called label stack, 3-bits are experimental bits often used for specifying class of service. One bit is reserved for bottom of stack bit and is set if no label follows. 8-bits are used for time-to-live (TTL) used in the same way like IP [3]

C. Label Distribution

A forwarding algorithm alone is not enough to implement an MPLS network. The individual nodes need to know the network topology in order to make informed forwarding decisions. Because MPLS is not tied to a particular paradigm, any routing protocol capable of carrying MPLS labels can be used to build MPLS LSPs. Such protocols include:

- **Label Distribution Protocol (LDP):** This protocol is designed to build aggregate LSPs based on IP routing information gathered by a traditional IP routing protocol such as RIP [1].
- **Resource Reservation Protocol (RRP):** Traffic Engineering (RSVPTE): This protocol incorporates extensions to RSVP in order to construct LSP tunnels along requested paths with varying QoS. RSVP-TE is commonly used for traffic engineering (TE) in MPLS networks [2].
- **Multiprotocol Extension to Border Gateway Protocol 4 (MPBGP):** This protocol extends BGP, and generalizes distributed gateway addresses and carries labels. It is commonly used to build VPNs [4].

V. HYPER SPEED DEFENSE ON DIFFERENT NETWORKS

A. Hyper speed Defense On Local Area Networks (LAN)

The same hyper speed communication process discussed may be applied to a LAN. Hyper speed signals are identified by reserving a special set of MAC addresses using fields in 802.1q (VLAN) headers or using 802. 1p (Ethernet QoS), depending on the technologies supported by Ethernet switches 26. To implement the hyper speed communications, most Ethernet switches 26 would require specialized software.

Implemented in a similar manner to hyper speed communications, queue priority is implemented by programming Ethernet switches 26 to forward hyper speed frames ahead of all other frames in the memory of Ethernet switches 26. Ethernet switches 26 supporting 802. 1p are already equipped for queue priority. Implementing delay variation includes programming Ethernet switches 26 to place non-hyper speed frames in a queue where the frames wait for a fixed period-of-time.

Route variation is implemented in several ways. One approach is to modify the Spanning Tree Protocol to calculate two spanning trees. The example in figs. 1A and 1B depicts two spanning trees in Ethernet LAN 28. A non-optimal spanning tree used by non- hyper speed frames is illustrated in fig. 1A. fig. 1B illustrates the minimum spanning tree, which is used by hyper speed frames. Lines 27 depict the Ethernet links. Dashed lines 27A indicate that the link has been selected as part of the spanning tree. The approach for implementing route variation is limited because the reaction time window provided by the maximum spanning tree compared to that provided by the minimum spanning tree may not be sufficient to implement defensive actions. This problem is resolved by also applying the delay variation technique to obtain the desired reaction time window.

Alternatively, implementing route variation involves programming Ethernet switches 26 to store the loop count in an unused Ethernet header field, and to send frames in loops a fixed number of times. Another alternative employs Virtual LAN (VLAN) 28 hopping. This alternative is also applicable to enterprise networks.

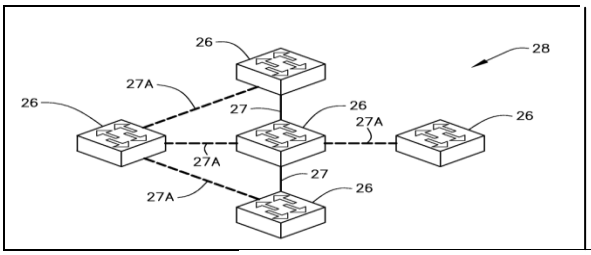

Fig. 1A.

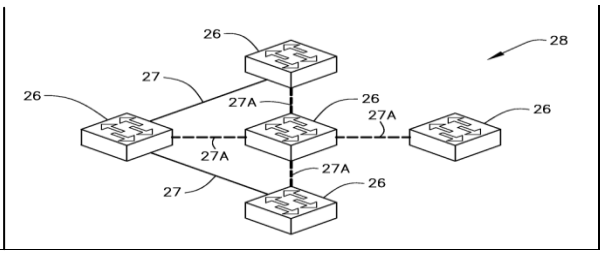

Fig. 1B.

B. Hyper speed Defense on Service Provider Networks

Referring to fig. 2, network 10, is illustrated as having nodes 12. Nodes 12 are represented as A-F. In this case network 10 is a service provider network 10. Node 12 A-F representations are associated with routers 14A-14F. Links 16 are the connections between nodes 12. In network 10, as illustrated, node 12A is the ingress node, and node 12F is the egress node. Node 12A is also referred to in fig. 2 as the source or origination node. Node 12F is also referred to as the termination node or destination node.

Route 18 is the sequence of links 16 that an electronic signal travels between an origination or source node 12A, and the intervening nodes 12B and 12C until it reaches a termination or destination node 12F. fig. 2 illustrates route 18 as three links 16 between nodes 12 marked as A-B-C-F, which are also routers 14A, 14B, 14C and 14F. Similarly, nodes 12D and 12E are also routers 14D and 14E. Path 20 includes links 16 and queues associated with nodes 12. Path 20 is illustrated in fig. 2 as three links 16 between and including nodes 12 marked as A-B-C-F, which are also routers 14A, 14B, 14C and 14F. The dashed line on fig. 2 represents path 20. The path time is the sum of the delay times imposed by the constituent links 16 and queues comprising path 20.

Network 10 illustrated in fig. 2 is representative of a multiprotocol label switching (MPLS) provider network. MPLS is an ideal technology for implementing hyper speed signalling because it has built-in identification and service differentiation technologies. Labels in MPLS act like circuit identifiers in asynchronous transfer mode (ATM) to designate paths 20 taken by packets in the core of network 10.

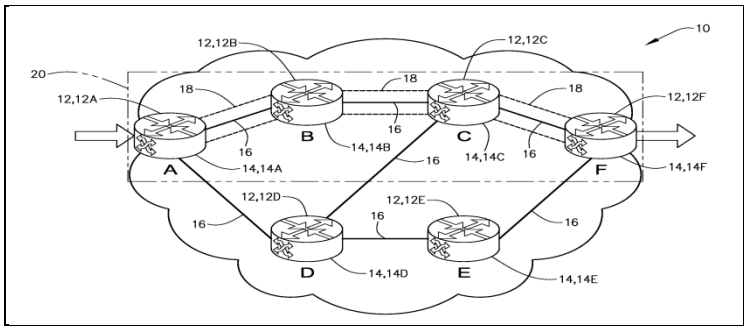

Fig.2 MPLS network

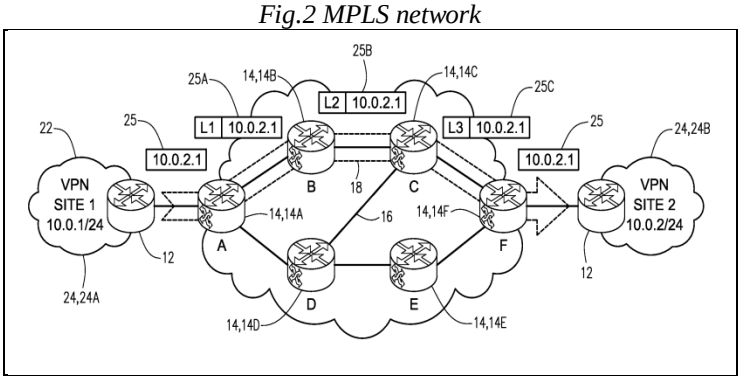

Fig.3 VPN

Virtual private network (VPN) 22, consisting of two sites 24, is connected via network 10 as illustrated in fig. 3. VPN 22 in fig. 3 is a prior art illustration as part of a VPN service provider. An unlabeled internet protocol (IP) packet 25 travelling from site 24A to site 24B enters network 10 at router 14A. Router 14A is referred to as label edge router (LER) 14A because it resides at the edge of an MPLS domain. LER 14A examines the destination IP address, consults its IP routing table, applies a Label LI thereto, and forwards packet 25 to router 14B. Router 14B is referred to as label switching router (LSR) 14B because it resides within the MPLS domain. LSR 14B is positioned to receive labelled IP packet 25 and detects Label LI . Using the Label LI, LSR 14B immediately identifies the path for packet 25, replaces Label LI with Label L2, and forwards packet 25 to LSR 14C. LSR 14C functions in a manner similar to LSR 14B, applies Label L3, and forwards packet 25 to LER 14F. LER 14F recognizes that packet 25 has reached the destination network, removes the label, and forwards the unlabeled IP packet 25 to site 24B.

Using fig. 3 as an example, hyper speed routing in MPLS uses labels to distinguish hyper speed packets 25 from non-hyper speed packets 25. MPLS-capable routers 14 are equipped with quality of service (QoS) and traffic shaping features. LSRs 14 are configured to give hyper speed packets 25 the highest priority based on the packet label. Likewise, LSRs are configured to delay hyper speed packets 25 for a fixed period-of-time in forwarding queues. A non-limiting example of a delayed period-of-time is about 50 milliseconds. Because the label dictates the QoS and path 20, non-hyper speed packets 25 can be redirected along circuitous routes 18 by constructing the corresponding paths 20 using non-hyper speed labels. The labels corresponding to optimal routes 18 are reserved for hyper speed packets 25.

C. Hyper speed Defense on Enterprise Networks

Referring to fig. 4, enterprise network is illustrated. Because enterprise networks 30 are composed of LANs 28 using IP, the techniques for implementing hyper speed signalling in LANs 28 are also applicable to enterprise networks 30. However, the protocols that support enterprise networks 30, such as IP, are manipulated to enable hyper speed signalling in enterprise networks 30. Larger enterprise networks 30 may apply the same service differentiation techniques used by service providers. Depending upon the size of enterprise network 30, by way of a non-limiting example, and either singly or in combination, the protocols used include, IP, MPLS, as well as other older and newer protocols.

The type of service (ToS) field or an IP option can be used to distinguish hyper speed packets 25 from other packets 25. The features of routers 14 of enterprise network 30 determine particular service differentiation techniques available. If routers 14 have the proper features, the queue priority and delay variation techniques are implemented by configuring routers 14 to give priority to hyper speed packets 25 and to delay non- hyper speed packets 25 in queues.

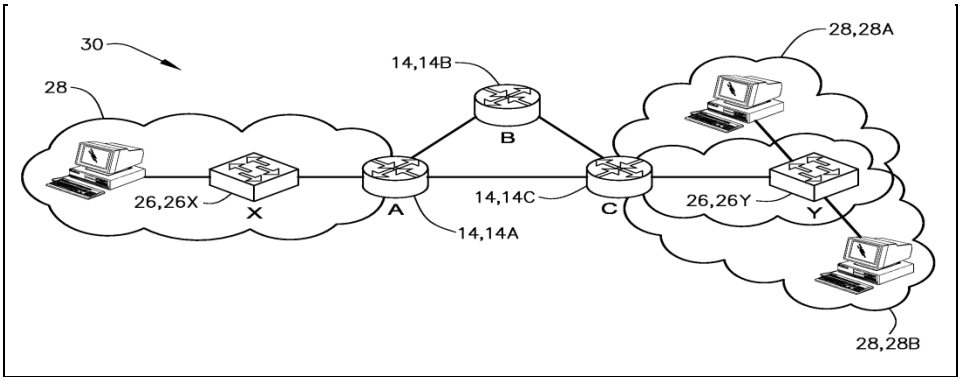

Fig. 4 Enterprise Network

Route variation is implemented by manipulating routing protocols (e.g., routing information protocol (RIP) and open shortest path first (OSPF)), or by applying a specialized hyper speed routing protocol such as Ac protocol, which is discussed in detail here in below. fig. 4 illustrates enterprise network 30 consisting of three LANs 28 connected by three IP routers 14. Two LANS 28A and 28B are both VLANs 28. To implement route variation, the routing table at router 14A must be manipulated, or router 14A must be programmed to send ordinary packets 25 to a next hop that does not correspond to the hyper speed path. Thus, hyper speed packets

travelling from LAN 28A to VLAN 28B follow the optimal hop sequence identified by X-A-C-Y. Non-hyper speed packets 25 follow the hop sequence identified by X-A-B-C-Y. Hop sequence X-A-C-Y represents Ethernet switch 26X to router 14A to router 14C to Ethernet switch 26Y. Similarly, hop sequence X-A-B-C-Y represents Ethernet switch 26X to router 14A to router 14B to router 14C to Ethernet switch 26Y. [0068] In the case of enterprise networks 30 employing VLANs 28, Ethernet switches 26 are programmed to permit VLAN 28 hopping. Referring to fig. 4, hyper speed packets 25 travelling from VLAN 28B to VLAN 28C hop via Ethernet switch 26Y without visiting router 14C. On the other hand, non-hyper speed packets 25 travel via the sequence of Y-C-Y, visiting router 14C as expected. The sequence of Y-C-Y represents packet travel from VLAN 28B to Ethernet switch 26Y to router 14C to Ethernet switch 26Y to VLAN 28C.

Enterprise networks 30 may contain VPNs 22. The implementation of hyper speed signalling in enterprise networks 30 with VPNs 22 that span multiple geographic locations may require the cooperation of one or more service providers.

D. Hyper speed Defense on Internet

When using hyper speed defense on internet, internet protocols require modification of the software in routers 14 and Ethernet switches 26. However, an altered protocol can be wrapped between service provider networks, LANs 28 and enterprise networks 30. Other switches used with computer communications, such as ATM switches, fiber optics, etc., are understood to be used in place of, or in combination with Ethernet switches 26. Hyper speed packets 25 in the Internet are identified using ToS or optional IP fields. Since the Internet is composed of service provider networks 10, hyper speed signalling implementations for service provider networks 10 are employed. The same is true of LANs 28 and enterprise networks 30. Enterprise networks, LANs, and participating providers perform hyper speed routing without the cooperation of non-participating providers. Non-participating providers behave in the standard way while participating networks treat the non-participating providers as if they were links among the participating networks.

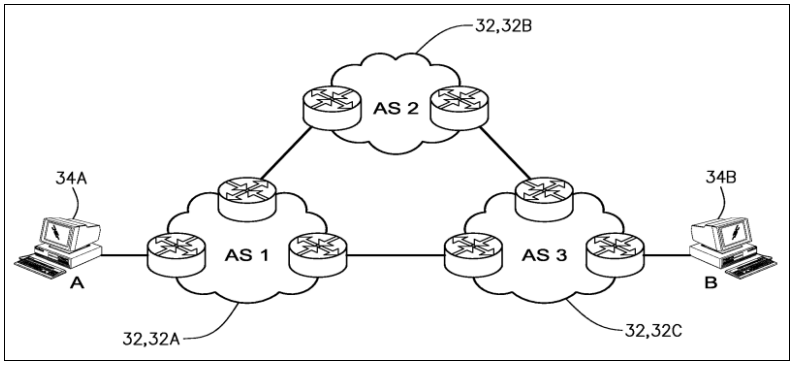

Fig. 5 Internet

Cooperating service providers can also manipulate the Border Gateway Protocol (BGP) to create optimal and suboptimal paths 20 without advertising the optimal (hyper speed) paths 20 to non-cooperating service providers. fig. 5 illustrates three autonomous systems (AS) 32 with Client 34A connected to AS 32A and Client 34B connected to AS 32C. Hyper speed packets 25 travelling from Client 34A to Client 34B would follow the AS 32 sequence of AS 32A to AS 32C, while non-hyper speed packets 25 would follow the AS 32 sequence of AS 32A to AS 32B to AS 32C.

VI. CONCLUSIONS

MPLS has emerged as a mainstay for transporting large volumes of traffic over a wide array of networks. Indeed, much of the world's enterprise traffic already depends on MPLS-based infrastructures to deliver reliable voice, video and application services. A persistent attack on the MPLS infrastructure could cripple corporate, national and even global operations. As attacks on computer and telecommunications networks become more prolific and more insidious, it will be increasingly important to deploy novel strategies that give the advantage to network defenders.

Hyper speed signaling is a promising defensive technology that could combat current and future threats. Hyper speed signaling does not require electrons to move faster than the laws of physics permit; instead, malicious traffic is slowed down ever so slightly to endow defensive capabilities that are seemingly magical. The

hallmark of good engineering is making the right trade-off. Intentionally slowing down network traffic may appear to be counterintuitive, but the defensive advantages gained by hyper speed signaling may well outweigh the costs.

REFERENCES

[1] Pure MPLS Technology, Availability, Reliability and Security. Botham, P. and Liwen, He. 2008. third international conference. pp. 253-259.

[2] Gray, E. MPLS: Implementing the Technology. Massachusetts, : s.n., 2001.

[3] MPLS Technology on IP Backbone network. Kumar, Dinesh and Karur, Gurpreet. 1, Aug 2010, International journal of Computer Applications, Vol. 5, pp. 13-16.

[4] Multiprotocol Extensions For BGP-4. Bates, T., et al. 2000, RFC 2858.

[5] Security analysis of RSVP-TE signaling in MPLS networks. Spainhower, M., et al. 2008, International Journal of Critical Infrastructure Protection, Vol. 1, pp. 68-74.

[6] Best, R. Intelligence, Surveillance and Reconnaissance (ISR) Programs:Issues for Congress. Congressional Research Service. Washington, DC : s.n., 2005. CRS Report for Congress.

[7] Peterson, L. and Davie, B. Computer Networks: A Systems Approach. [ed.] Morgan Kaufmann. San Francisco : s.n., 2003.

[8] IMPLEMENTING NOVEL DEFENSE FUNCTIONALITY IN MPLS NETWORKS USING HYPERSPEED SIGNALING. Guernsey, Daniel, Rice, Mason and Shenoi, Sujeet. [ed.] Jonathan Butts and Sujeet Shenoi. Hanover, NH, USA : Springer, 2011. International Conference on Critical Infrastructure Protection. Vol. 5, pp. 91-106. ISSN 1868-4238, ISBN 978-3-642-24864-1, e-ISSN 1868-422X, e-ISBN 978-3-642-24864-1.

[9] Shenoi, Sujeet, Guernsey, Daniel and Rice, Mason. Network-based hyperspeed communication and defense . WO2012115679 A1 US, Aug 30, 2012. Application.

