Ergebnisse einer neuen Untersuchungsmethode zur Messung der Störempfindlichkeit von Ethernetverbindungen

Dipl.-Ing. Matthias Kreitlow, Wehrwissenschaftliches Institut für Schutztechnologien – ABC-Schutz, Geschäftsfeld Elektromagnetische Wirkungen und HPEM
Prof. Dr.-Ing. Heyno Garbe, Leibniz Universität Hannover, Institut für Grundlagen der Elektrotechnik und Messtechnik
Dr.-Ing. Frank Sabath, Wehrwissenschaftliches Institut für Schutztechnologien – ABC-Schutz, Geschäftsbereich Kernwaffenwirkungen, HPEM, Brandschutz

1. Einleitung und Motivation

Datennetzwerke sind heutzutage überall anzutreffen. Ihr Einsatzgebiet reicht vom Heimgebrauch über industrielle Anwendungen bis hin zur militärischen Nutzung. Eine weit verbreitete Technik stellt dabei das Ethernet nach IEEE 802.3 Clause 40 (1000BASE-T) mit einer Übertragunsrate von 1000 MBit/s – meist auch schlicht als „Gigabit-Ethernet“ bezeichnet – dar.

Die eingesetzten Twisted-Pair-Kabel stellen aufgrund ihrer metallischen Ausführung einen Einkopplungspfad für elektromagnetische Störungen dar [1]. Gerade beim Einsatz in kritischen Infrastrukturen oder rauen Umgebungen wie Industrieanlagen oder Schiffen stellt sich daher die Frage nach der Störempfindlichkeit solcher Netzwerke. Hier kommt insbesondere als Störquelle nicht nur die normale EMV-Umgebung in Betracht, sondern auch künstliche Störquellen, welche vorsätzlich elektromagnetische Felder hoher Leistung erzeugen.

Bei Betrachtung der Störempfindlichkeit sind unerwünschte Einflüsse auf die Datenübertragung und die zugrunde liegenden Fehlermechanismen von besonderem Interesse, da hier Einflüsse schon feststellbar sind, bevor die Ausfallschwellen der beteiligten Komponenten erreicht werden [2]. Um quantifizierbare Untersuchungen durchführen zu können, muss eine geeignete Testumgebung geschaffen werden. Diese besteht dabei aber nicht ausschließlich aus der Hardware der Netzwerkkomponenten und Computer, sondern auch aus der eingesetzten Software.

Da insbesondere höhere Protokollschichten dabei in Software realisiert sind, sind auch informationstechnische Elemente von induzierten Fehlern betroffen. Hierbei führt aber gerade erst das vorgesehene Verhalten dieser höheren Schichten zu bestimmten wahrnehmbaren Fehlereffekten auf der Anwendungsebene. Es ergibt sich also nur ein mittelbarer Zusammenhang mit der Störeinwirkung, sodass die eigentlichen physikalischen Störungseinflüsse auf dem Netzwerkmedium auf Anwendungsebene ohne weiteres kaum genau erfasst werden können.

Ziel dieser Arbeit ist die Vorstellung der Ergebnisse einer neuen Messmethode, welche bisher unbeachtete Software-Effekte berücksichtigt und diese umgeht. Damit können auf Anwendungsebene einfach zu erzeugende Messergebnisse auf die tatsächlichen physikalischen Wechselwirkungen mit dem Netzwerkmedium zurückgeführt und mit diesen in

ISBN 978-3-8007-3577-8

quantitativen Zusammenhang gebracht werden. Ebenso kann der Einfluss einzelner Software-Parameter bestimmt werden. Die Interpretation der Ergebnisse führt zu neuen, bisher durch höhere Protokollschichten überdeckten Effektmechanismen [3].

2. Entwurf eines Test-Setups

2.1 Aufbau eines generischen Test-Netzwerkes

Um die Störempfindlichkeit von Ethernetverbindungen zu ermitteln, muss zunächst eine geeignete Testumgebung eingerichtet werden. Diese besteht neben Computern als Kommunikationspartnern auch aus Switchen und Netzwerkkabeln. Bild 1 zeigt schematisch das Test-Setup, welches eine verzweigte Netzwerktopologie wie etwa an einem Flughafen in generischer Weise abbildet.

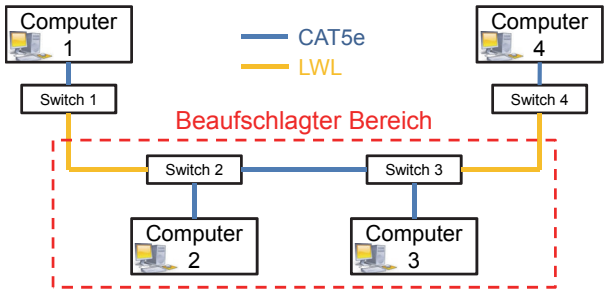

Bild 1: Netzwerk-Setup

Der beaufschlagte Teil des Netzwerkes ist hierbei durch die Verwendung von optischen Netzwerkverbindungen (LWL) elektrisch vom restlichen Teil getrennt, sodass Störungen nur mit den Komponenten innerhalb des beaufschlagten Bereiches physikalisch in Wechselwirkung treten können. Ebenfalls ist die Stromversorgung der beaufschlagten und nicht beaufschlagten Komponenten voneinander isoliert.

Diese Netzwerktopologie ermöglicht die Untersuchung verschiedener Anwendungsszenarien: Datenübertragung

1. durch den gestörten Bereich (PC1 – PC4),
2. in den gestörten Bereich (PC1 – PC2),
3. aus dem gestörten Bereich (PC3 – PC4),
4. innerhalb des gestörten Bereichs (PC2 – PC3).

Hierdurch ist es möglich, unterschiedliche Störeffekte bei einer reinen Beeinflussung der Datenleitungen sowie bei einer Beeinflussung von Computern separat zu identifizieren.

2.2 Entwicklung einer Test-Applikation

Um die Auswirkungen von Störungen auf Datenübertragungen zu bestimmen, können verschiedene Ansätze verfolgt werden. Mittlerweile kommt in fast allen Netzwerken das Internet-Protokoll (IP) zum Einsatz, auf das entsprechende Anwendungen aufsetzen.

Ein sehr einfach anzuwendendes Verfahren zur Überprüfung der Erreichbarkeit eines Ziel-Systems stellt der ICMP-Echo-Request dar, welcher auf nahezu jedem Betriebssystem mit dem Programm „ping“ abgesetzt werden kann. Hierbei sendet ein Netzwerkteilnehmer zu einem anderen eine Anfrage („ping“), dieser antwortet darauf hin mit einer Wiederholung der Anfrage („pong“). Bei einer Unterbrechung der Verbindung erhält der

ISBN 978-3-8007-3577-8

anfragende Computer keine Antwort mehr. Dieses Verfahren erlaubt jedoch lediglich die Detektion einer Unterbrechung, aufgrund des geringen Datenvolumens und der niedrigen zeitlichen Auflösung ist jedoch keine exakte Quantifizierung von Störungsereignissen möglich.

Andere Messmethoden versuchen, den Störungsgrad einer Netzwerkverbindung über den erreichbaren Durchsatz bei einer Datenübertragung heranzuziehen. Hierzu wird mittels einer geeigneten Applikation – etwa einem FTP-Server/Client – versucht, eine hohe Auslastung im Netzwerk erzeugen. Das Verhalten der Datenübertragungsrate im Störungsfall wird als Maß für die Störung der Netzwerkverbindung herangezogen. Diese Methode ist jedoch mit deutlichen Nachteilen behaftet. So beruhen übliche Applikationen zur Datenübertragung auf dem Transmission-Control-Protocol (TCP). TCP implementiert hierbei zum einen eine Sicherungsschicht, welche eine fehlerfreie und vollständige Datenübertragung über beliebige Medien sicherstellen soll. Zum anderen steuert dieses Protokoll auch den Datenfluss, um in Konkurrenzsituationen oder bei Engpässen wegen zu geringer Übertragungskapazität regelnd eingreifen zu können.

Wird also ein Datentransfer gestört, sodass sich Datenfehler oder -verluste während der Übertragung ergeben, so wird genau dieser Umstand von TCP erkannt und entsprechende Regelungsmechanismen setzen ein. Dies umfasst u.a. eine Anpassung der Sende- und Empfangspuffer („TCP-Receive-Window“), wiederholtes Senden von Daten („Retransmissions“) oder das Anpassen von Zeitfenstern („Timeouts“). Dies führt dazu, dass die Datenrate automatisch reduziert wird, da das System von einer Überlastung der Datenverbindung ausgeht. Insbesondere bei repetitiven Störungen ist dieser Effekt sehr deutlich.

Für eine Beurteilung der Störung ist dieser Umstand von außerordentlichem Nachteil. Es wird zwar die tatsächliche Auswirkung auf eine Anwendung erfasst, diese steht jedoch nur in einem mittelbaren Zusammenhang mit den unerwünschten Wechselwirkungen der beteiligten Systeme und Übertragungswege. Die zu beobachtende Reduzierung der Datenrate ist ein wesentlicher Effekt durch das gewollte Verhalten höherer Netzwerkschichten. Auch zu beobachtende Verbindungsabbrüche stehen nicht direkt in Zusammenhang mit einer physikalischen Störeinwirkung, sondern sind Software-induziert. Hier entscheiden Timeouts, wann eine Verbindung als abgebrochen gilt.

Aus diesen Gründen wurde für die durchgeführten Experimente ein neues Verfahren implementiert, welches als Applikation auf einem Computer eingesetzt werden kann und zugleich eine direkte Einwirkung von Störungen auf dem Netzwerkmedium quantitativ bestimmbar macht. Dieses Programm arbeitet nach einem klassischen Client-Server-Prinzip, wobei ein Computer die Anforderung für einen Datenstrom an einen anderen Computer sendet und daraufhin diese Daten vom anderen Computer empfängt.

Im Gegensatz zu klassischen Anwendungen wie einem FTP-Client/Server wurde in dem Messprogramm jedoch bewusst auf die Verwendung eines gesicherten Verbindungsprotokolls wie TCP/IP verzichtet. Vielmehr erzeugt der sendende Computer einen definierten und genau vorhersagbaren Datenstrom, von dem der empfangende Computer alle tatsächlich korrekt empfangenen – also nicht gestörten – Datenpakete aufzeichnet. Damit kann eine unerwünschte Einflussnahme von nur schwer determinierbaren Fehlerkorrektur- oder Flusssteuerungsalgorithmen ausgeschlossen werden. Die Identifikation von Störungen und deren Auswirkungen erfolgt durch eine nachträgliche Auswertung der tatsächlich empfangenen Daten.

ISBN 978-3-8007-3577-8

3. Experimentelle Untersuchungen

3.1 Messaufbau

Mit Hilfe des zuvor genannten Testverfahrens wurden Untersuchungen am skizzierten Test-Setup durchgeführt. Der beaufschlagte Bereich wurde dabei wie in Bild 2 gezeigt mit einer Ultra-Breitband-Quelle (UWB) bestrahlt. Die UWB-Quelle bestand aus dem Impulsgenerator PBG-7 und einer Hornantenne.

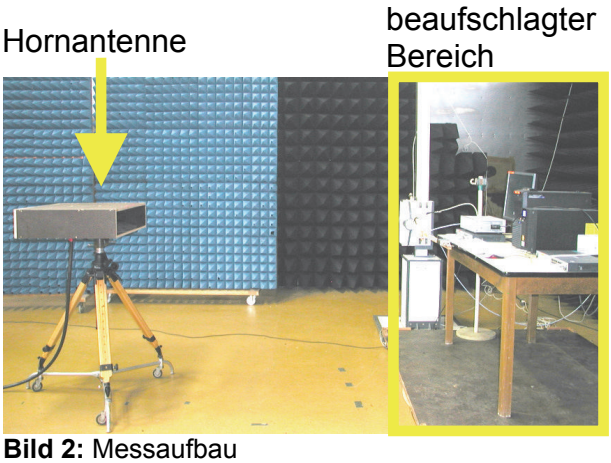

Bild 2: Messaufbau

Die gesamte Installation befand sich auf einem metallfreien Holztisch über normalem Betonboden. Die Umgebung war mit Pyramidenabsorbern ausgekleidet, um unerwünschte Reflexionen des elektromagnetischen Feldes zu verhindern.

Das Feld wurde an der Vorderseite des Versuchsaufbaus im bestrahlten Bereich mit einer differenzierenden Feldsonde ermittelt. Die Feldstärke an den Versuchsobjekten lag bei 7,5 kV/m mit vertikaler Polarisation bei einer Anstiegszeit von 150 ps. Die Pulswiederholrate (PRF) wurde von 0 Hz (entspricht keiner Beaufschlagung) bis 800 Hz variiert. Bild 3 und 4 zeigen einen Feldpuls im Zeit- und Frequenzbereich.

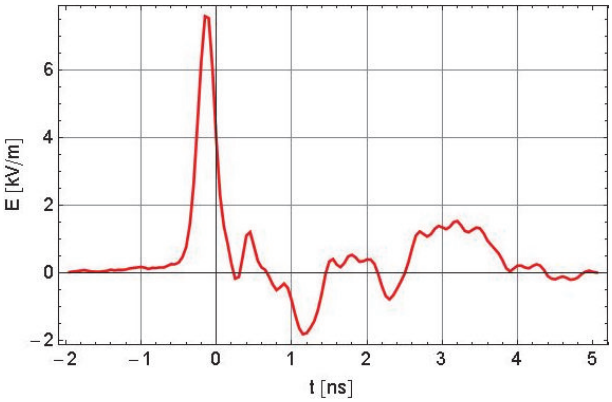

Bild 3: Feldpuls im Zeitbereich

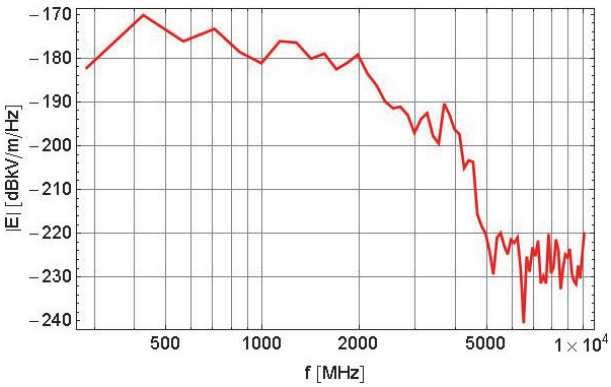

Bild 4: Feldpuls im Freuqenzbereich

Bei diesen Versuchsparametern war sichergestellt, dass die Ausfallgrenze der eingesetzten Netzwerk-Komponenten noch unterschritten war, aber bereits Einflüsse auf die Datenkommunikation feststellbar waren.

3.2 Versuchsdurchführung

Der Ablauf der Messungen gestaltete sich nach einem festen Schema. Zunächst wurde zu Beginn jeder Messreihe eine Messung des ungestörten Falls (PRF = 0 Hz) durchgeführt, um einen ordnungsgemäßen und reproduzierbaren Systemzustand nachzuweisen. Für die ersten beiden Messreihen (siehe 4.1 und 4.2) wurden IP-Datenpakete mit 1472

ISBN 978-3-8007-3577-8

Bytes Nutzdaten gesendet. Dies führt zu den größtmöglichen Ethernetrahmen von 1538 Bytes Länge, sodass die Datenpakete gerade noch nicht fragmentiert werden müssen. Die Länge einer Datenübertragung betrug immer 40 Sekunden, wobei eine Störbeaufschlagung immer 10 Sekunden nach Beginn der Übertragung für 20 Sekunden stattfand. Die gewählten Netzwerkparameter führen zu einer Paketrate von ca. 5000 Pakten/Sekunde, was einer Bruttodatenrate von ca. 7,5 MByte/Sekunde und einer Netzwerkauslastung von ca. 6% entspricht. Pro Experiment wurden exakt 200581 Datenpakete gesendet. Für die Messungen unter 4.3 wurde die Paketgröße auf 65112 Bytes angehoben, wodurch die Auslastung auf ca. 64% stieg.

Bei den Experimenten wurden zwei Fälle betrachtet. Im ersten sollten die reinen Auswirkungen auf die Übertragungstrecke bestehend aus Datenleitungen und Switchen untersucht werden (siehe 4.1). Im zweiten sollte das Verhalten von Datenübertragungen untersucht werden, wenn ein an der Kommunikation beteiligter Computer der Störbeaufschlagung ausgesetzt ist (siehe 4.2, 4.3).

Hierzu wurde in einer ersten Versuchsreihe eine Datenübertragung von Computer 1 zu Computer 4 initiiert und das System währenddessen beaufschlagt. Die Daten liefen dabei im bestrahlten Bereich über die Switche 2 und 3 sowie die CAT5e-Leitung, während Computer 1 und 4 nicht gegenüber dem Feld exponiert waren.

Bei den anschließenden Experimenten wurde eine Datenübertragung von Computer 3 zu Computer 4 durchgeführt, sodass hier neben dem exponierten Übertragungsweg auch der sendende Computer durch das elektromagnetische Feld beaufschlagt war.

4 Messergebnisse

4.1 Empfindlichkeit der Übertragungsstrecke

Der zeitliche Verlauf der Datenübertragungsrate ist in Bild 5 dargestellt. Bild 6 zeigt die Anzahl an fehlenden Datenpakten während einer Datenübertragung.

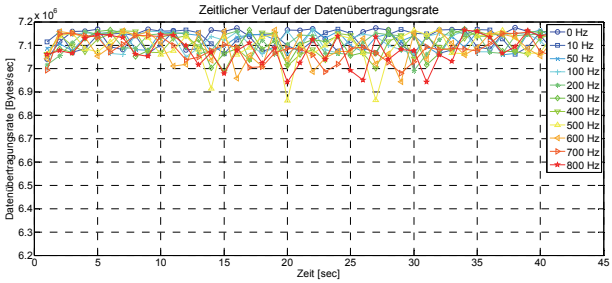

Bild 5: Verlauf der Datenrate (PC1-PC4)

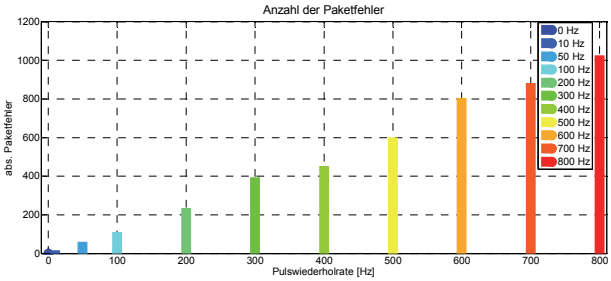

Bild 6: Anzahl an Paketfehlern (PC1-PC4)

Während anhand der erreichten Datenübertragungsrate in Bild 5 kaum eine Auswirkung feststellbar ist, so lässt sich an der Anzahl der fehlenden Datenpakete in Bild 6 der Störeinfluss erkennen. Es besteht ein linearer Zusammenhang zwischen der PRF und der Anzahl an fehlerhaften Datenpaketen. Diese steigt von Null im ungestörten Fall bis zu etwa 1000 Fehlern bei 800 Hz PRF linear an. Die absolute Anzahl an fehlerhaften Datenpaketen ist jedoch gegenüber der Gesamtzahl an übertragenen Paketen sehr gering, worin letztlich der geringe Einfluss auf die Übertragungsgeschwindigkeit begründet liegt.

ISBN 978-3-8007-3577-8

4.2 Empfindlichkeit von Computern

Wird ein Computer beaufschlagt, der an der Datenübertragung beteiligt ist, verändern sich die auftretenden Effekte deutlich. Sowohl an der Datenrate in Bild 7 als auch an der Anzahl der Paketfehler in Bild 8 ist nun die Störeinwirkung erkennbar.

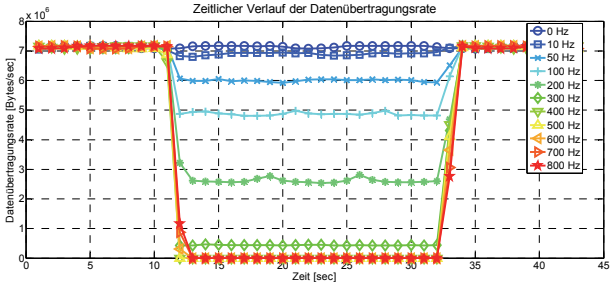

Bild 7: Verlauf der Datensrate (PC3-PC4)

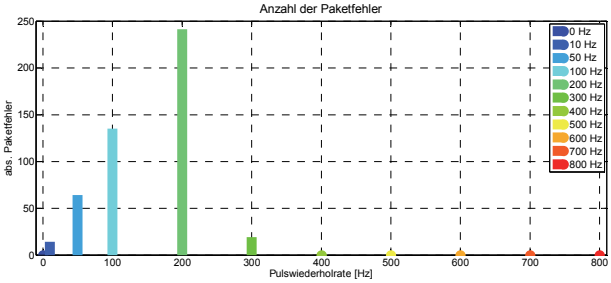

Bild 8: Anzahl an Paketfehlern (PC3-PC4)

Zunächst zeigt sich ein deutlicher Einbruch der Datenrate bei einer Störbeaufschlagung. Dabei verhält sich die Reduzierung der Datenrate linear zur PRF im Bereich bis 300 Hz. Ab einer PRF von 400 Hz kommt es für die Dauer der Störbeaufschlagung zu einer vollständigen Unterbrechung der Datenübertragung, die jedoch nach Ende der Störeinwirkung mit voller Geschwindigkeit weiterläuft.

Die Anzahl an Paketfehlern spiegelt dieses Verhalten nur eingeschränkt wieder. Die absolute Anzahl an Fehlern steigt bis zu einer PRF von 200 Hz zwar zunächst linear an, die Fehlerzahl liegt jedoch deutlich unter den Messungen der vorigen Versuchsreihe. Der weitaus stärkere Einbruch der Datenübertragungsgeschwindigkeit hätte hier eine höhere Fehlerzahl erwarten lassen. Ab einer PRF von 300 Hz sinkt die Anzahl der absoluten Paketfehler auf bis zu Null ab, obgleich eine Datenübertragung nicht mehr möglich erscheint. Es muss also ein anderes Phänomen zu einer Herabsetzung der Datenübertragungsrate führen.

Das eingesetzte Messverfahren erlaubt es, die Datenübertragung bis auf Paketebene aufzulösen. Bild 8 zeigt einen Ausschnitt aus dem zeitlichen Verlauf der Datenübertragungsrate bei einer PRF von 100 Hz.

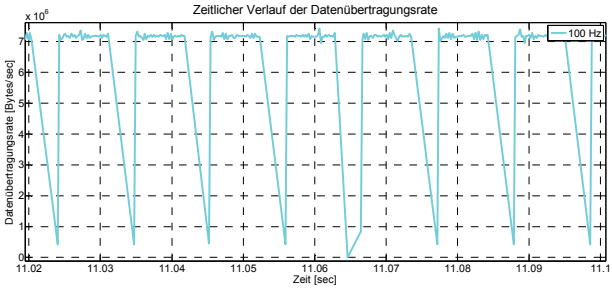

Bild 9: Ausschnitt aus Bild 7 (PRF = 100 Hz)

Aus diesen hoch aufgelösten Messdaten geht hervor, dass jeder Störimpuls das Senden von Daten in den meisten Fällen nur kurzzeitig verzögert, was maßgeblich zu einer Reduzierung der Übertragungsgeschwindigkeit führt. Nur vereinzelt bricht die Datenrate auf Null zusammen, was einem tatsächlich gestörten Paket entspricht.

Bei weiter steigender PRF kommt es immer häufiger zu einer Verzögerung des sendenden Computers, bis schließlich für die Dauer der Störübertragung keine Daten mehr übertragen werden können. Gleichzeitig bedeutet aber auch eine reduzierte Sendegeschwindigkeit, dass weniger bzw. gar keine Pakete übertragen und somit gestört werden können. Dieses Verhalten spiegelt das Histogramm in Bild 8 wieder.

ISBN 978-3-8007-3577-8

4.3 Einfluss von Protokollparametern

Die letzte Messreihe wurde nochmals mit geänderten Protokolleinstellungen wiederholt. Dabei wurde die Größe eines Datenpaketes auf 65112 Bytes erhöht, was zu einer wesentlich höheren Netzwerkauslastung führt. Ebenfalls gemessen wurden wiederum die Anzahl an fehlenden Datenpaketen sowie der zeitlicher Verlauf der Datenübertragungsrate. Letzte ist in diesem Fall von besonderem Interesse. Entspricht die Fehlerzahl bei diesem Experiment dem Ergebnis aus Bild 8, hat die Datenübertragungsrate den Verlauf aus Bild 10.

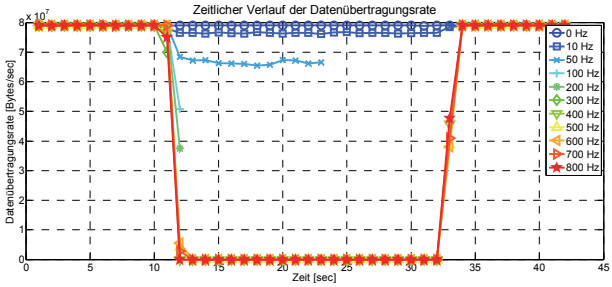

Bild 10: Verlauf der Datenrate (PC3-PC4, 65112 Bytes)

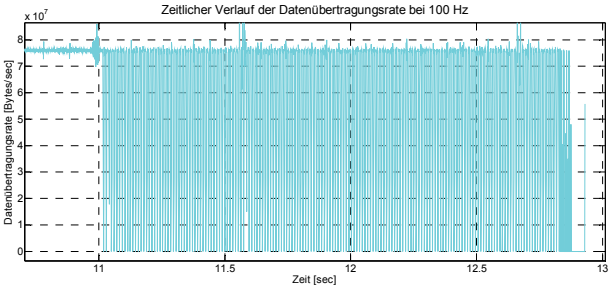

Bild 11: Ausschnitt aus Bild 10 (PRF = 100 Hz)

Der Grafik ist zu entnehmen, dass die Datenübertragung bei einer PRF von 50 Hz bis 300 Hz nach kurzer Zeit abbricht und auch nach Ende der Störbeaufschlagung nicht weiterläuft. Ab einer PRF von 400 Hz kommt es zu einer wie im vorherigen Experiment beobachteten Unterbrechung mit anschließendem Fortlaufen der Übertragung.

Um dieses Verhalten zu erklären, kann abermals eine auf Paketebene aufgelöste Darstellung in Bild 11 herangezogen werden. Hier ist deutlich zu erkennen, dass es nicht augenblicklich zu einem Abbruch kommt, sondern die Datenübertragung für eine gewisse Zeit zunächst mit dem aus Abschnitt 4.2 bekannten Fehlerbild weiterläuft. Erst dann kommt es zu einem vermeintlichen Abbruch. Die Beobachtung der Switche und auch eines Netzwerkmonitors auf dem empfangenden und nicht bestrahlten Computer hat aber ergeben, dass auch nach diesem vermeintlichen Abbruch weiterhin Daten auf diesem Computer eintreffen.

Hier handelt es sich um einen Software-induzierten Fehler auf der Vermittlungsschicht. Die Größe der Datenpakete von 65112 Bytes macht es notwendig, diese Pakete in kleinere zu fragmentieren. Diese müssen am empfangenden Rechner wieder zusammengesetzt werden, bevor das Datenpaket für die Anwendung zu Verfügung steht. Gehen nun einzelne Fragmente durch eine Störbeaufschlagung verloren, können diese Pakete nicht vervollständigt werden und verharren in einem Software-Puffer (sog. „IP Reassembly Cache“), in dem die Fragmente zwischengespeichert werden.

Dieser Puffer ist von endlicher Größe, sodass ab Erreichen einer bestimmten Grenze von zwischengespeicherten, unvollständigen Datenpaketen keine neuen mehr vom TCP/IP-Protokollstapel verarbeitet werden können. Dies äußert sich in einem scheinbaren Abbruch der Verbindung auf Anwendungsebene, obgleich das Netzwerk physisch weiterhin in der Lage ist, Daten zu übertragen. Bemerkenswert ist, dass dieser Fehler erst auf dem empfangenden Rechner entsteht, der keiner elektromagnetischen Störeinwirkung ausgesetzt ist.

ISBN 978-3-8007-3577-8

5. Zusammenfassung

Zur Analyse der Störung von Ethernetverbindungen wurde eine neue Untersuchungsmethode angewandt, die das Verhalten von höheren Netzwerk-Protokollen mit berücksichtigt. Diese hat gezeigt, dass Effekte und Fehlermechanismen auftauchen, die durch einfache Tests mittels Durchsatzmessung mit Hilfe bekannter Anwendungen wie einem FTP-Client/Server nicht aufgedeckt werden können.

In keinem untersuchten Fall kam es zu einem nachhaltigen Abbruch der Ethernetverbindung. Dies lässt den Schluss zu, dass in anderen Untersuchungen beobachtete Verbindungsabbrüche nicht durch physikalische Fehler verursacht werden, sondern auf übergeordneten Netzwerk-Schichten entstehen. Dieses konnte bespielhaft durch die Variation der IP-Paketgröße, bei der es sich um einen Software-Parameter handelt, gezielt hervorgerufen werden. Die Ethernetverbindung bleibt jedoch weiterhin bestehen.

Der eigentliche Störungsgrad der Verbindung hängt dabei maßgeblich von der PRF ab. Hier konnte gezeigt werden, dass es bei einer reinen Störung des Übertragungsweges eine lineare Abhängigkeit der auftretenden Paketfehler zur PRF gibt. Selbst bei 800 Hz ist die Anzahl der Fehler gegenüber der Gesamtzahl an Datenpaketen jedoch so gering, dass sich kein signifikanter Effekt in der Datenübertragungsrate ergeben hat. Hieraus lässt sich schließen, dass die Auswirkungen eines einzelnen Störimpulses auch nur von kurzer Dauer sind, mit einer höheren PRF im kHz-Bereich aber deutlichere Störungen zu erwarten sind.

Ein anderes Fehlerbild ergibt sich bei der Störbeaufschlagung von Computern während einer Datenübertragung. Hier konnte mit Hilfe der neuen Untersuchungsmethode festgestellt werden, dass es einen sehr starken Einfluss auf die erzielbare Datenübertragungsgeschwindigkeit gibt. Dieser geht jedoch nicht mit einer höheren Zahl an Paketfehlern einher, sondern liegt in einem verzögerten Senden von Daten durch den Computer begründet, was sogar zu einer Verringerung an gestörten Paketen führt.

Die Arbeiten wurden im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Projektes EMSIN (Elektromagnetischer Schutz von Verkehrsinfrastrukturen, Förderkennzeichen 13N10408) durchgeführt.

6. Literatur

[1] D.Nitsch, M.Camp, F.Sabath, J.L.Haseborg, H.Garbe, „Susceptibility of Some Electronic Equipment to HPEM Threats", Electromagnetic Compatibility, IEEE Transactions on, vol. 46, no. 3, August 2004, pp. 380-389

[2] Jeffrey, I.; Gilmore, C.; Siemens, G.; LoVetri, J., "Hardware invariant protocol disruptive interference for 100BaseTX Ethernet communications", Electromagnetic Compatibility, IEEE Transactions on, vol.46, no.3, August 2004, pp. 412,422

[3] van Leersum, B.J.A.M. and Buesink, F.J.K. and Bergsma, J.G. and Leferink, F.B.J. (2013) Ethernet susceptibility to electric fast transients. In: Proceedings of the 2013 International Symposium on Electromagnetic Compatibility (EMC Europe), 2-6 Sept 2013, Brugge, Belgium. pp. 29-33.

ISBN 978-3-8007-3577-8