Informatik und Physiologie

Die virtuelle Ratte

Der Tag, an dem die Nobelpreise für das Jahr 2014 übergeben wurden, war auch für Prof. Dr. Gabriele Peters und Dipl.-Inform. Jochen Kerdels ein besonderes Datum: Edvard und May-Britt Moser erhielten zusammen mit dem US-Amerikaner John O'Keefe den Nobelpreis für Physiologie und Medizin. Die Leiterin des Lehrgebiets Mensch-Computer-Interaktion der FernUniversität in Hagen und ihr Wissenschaftlicher Mitarbeiter haben Daten aus neurophysiologischen Studien des norwegischen Forscherehepaars Moser für ihre eigenen Grundlagenforschungen verwendet. Diese könnten einmal in der Gehirnforschung eingesetzt werden.

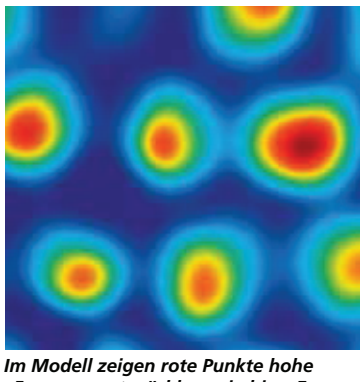
Der Physiologe Edward C. Tolman erkannte Ende der 1940er Jahre, dass Ratten ein zielgerichtetes Verhalten zeigen, wenn sie sich in einem Labyrinth bewegen. Seine Theorie: Ratten haben „eine Karte im Kopf", mit der sie „navigieren". Ein erster Hinweis darauf, dass Tolman recht haben könnte, wurde erst 1971 von John O'Keefe gefunden. Er identifizierte durch die direkte Messung einzelner Nervenzellen im Hippocampus von Rattenhirnen sogenannte „Ortszellen" („Place Cells"). Diese Neuronen wurden immer dann aktiv, wenn das Tier an bestimmten Stellen in einem Raum war. Jede Ortszelle war hierbei nur für einen bestimmten Teil des Raumes zuständig, andere Zellen „feuerten" an anderen Stellen. Eine Gruppe von Ortszellen stellt somit eine Art Karte dar – ganz so, wie Tolman es vorhergesagt hatte. Daraus ergaben sich neue Fragen: Woher „weiß" die „Ortszelle", wo die Ratte gerade ist? Welche Fähigkeiten müssen diese Zellen haben? Wie kann man sie zu einem bestimmten Verhalten anregen?

Virtuelles Koordinatennetz

Das Ehepaar Moser fand im Jahr 2005 sogenannte „Gitterzellen" („Grid Cells") in einem Bereich des Gehirns, der dem Hippocampus vorgeschaltet ist und der diesem Informationen zuführt. Gitterzellen werden an regelmäßigen Positionen im Raum aktiv und erzeugen mit dieser Aktivität ein virtuelles Koordinatennetz aus gleichseitigen Dreiecken.

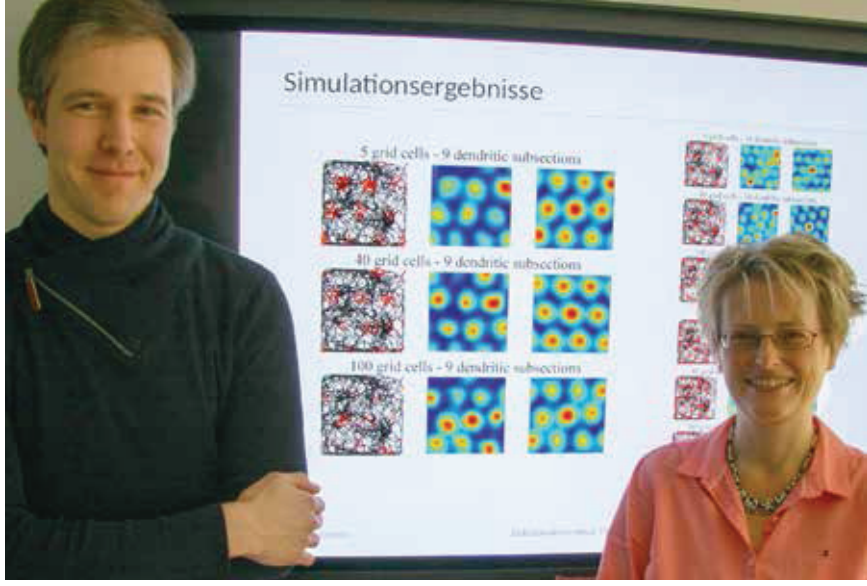
Dieses Muster weckte das Interesse des FernUni-Forschungsteams, da ähnliche Muster in der Informatik bei „selbstorganisierenden Lernverfahren" zu beobachten sind. Dementsprechend wurde auf Basis dieser Verfahren ein theoretisches Modell der Gitterzellen entwickelt. Wie in der Neurowissenschaft üblich stellten die Mosers die Daten ihrer Experimente der Wissenschaft zur Verfügung. Mit ihnen „fütterte" das Hagener Lehrgebiet sein theoretisches Modell. Wie ihr biologisches Vorbild „feuerte" auch die simulierte Zelle an regelmäßigen Positionen: Im Hagener Modell zeigte sich ebenfalls die Zerlegung des Raums in dreieckige Strukturen. Dies lässt vermuten, dass der Aktivität von Gitterzellen ein Prozess zur Fehlerminimierung zugrunde liegt.

Mit dem Modell können Gabriele Peters und Jochen Kerdels auch die Aktivität einer ganzen Population von Gitterzellen simulieren und erforschen, wie sich die Aktivitätsmuster der Zellen verändern, wenn man bestimmte Eigenschaften der simulierten Zellen verändert. Wie hängen zum Beispiel die Aktivitätsmuster der Gitterzellen



Im Modell zeigen rote Punkte hohe „Feuerungsraten", blaue niedrige. Es ergeben sich dreieckige Feuerungsgitter.

von der Struktur der Eingabedaten ab? Und können die Aktivitätsmuster anderer Neuronenarten mit dem gleichen Modell beschrieben werden?



Prof. Gabriele Peters und Jochen Kerdels

Zentrale neue Annahme des Lehrgebiets ist, dass der Dendritenbaum einer Zelle nicht einfach nur Informationen sammelt, sondern eine komplexere Aufgabe erfüllt – er wird daher von dem Hagener Forschungsteam als „selbstorganisierende Karte" betrachtet. „Vor kurzem publizierte Ergebnisse aus der Neurobiologie stützen diese These", so Projektleiter-Jochen Kerdels. Ein Dendritenbaum ist von seinem Aussehen und seiner Funktion her einer Baumwurzel ähnlich. Nur sammelt er Informationen und keine Nährstoffe. Je nachdem, welche Reize ihn treffen und an welcher Stelle dies geschieht, wird die Zelle dazu angeregt, auf verschiedene Eingabemuster zu reagieren. Vorherige Modelle gingen bislang davon aus, dass ein Neuron nur auf ein einzelnes Eingabemuster reagiert.

Der Erforschung von Gitterzellen kommt eine besondere Bedeutung zu, da sie in einem Hirnareal liegen, das mit hohen Gehirnfunktionen wie dem Abspeichern persönlicher Erlebnisse („episodisches Gedächtnis"), dem Orientierungssinn oder auch der Verarbeitung von Sprache in Verbindung steht: „Man lernt dadurch etwas über Hirnfunktionen und nähert sich ein wenig der Antwort auf die Frage, was Bewusstsein ist", erläutert Gabriele Peters.

Die Hagener sind sich darüber im Klaren, dass kurzfristig kaum praktische Anwendungsmöglichkeiten ihrer Grundlagenforschung zu erwarten sind. Das Modell könnte vielleicht in der Zukunft für bestimmte Krankheiten wie z.B. Demenz interessant werden: Was passiert, wenn mehr und mehr Neuronen absterben? Was, wenn der Dentridenbaum nur noch halb so lang ist? „Vielleicht kann man einmal voraussagen, wie sehr frühe Ausfallerscheinungen aussehen." Dafür muss das Modell, das sich heute nur auf eine bestimmte Art von Eingabedaten – dem Bewegungsmuster von Ratten – bezieht, auf andere Gebiete übertragen werden.

Die gewonnenen Vorhersagen können dann von der Neurobiologie praktisch überprüft werden. Prof. Peters unterstreicht, dass sie und ihr Team sich nicht als erste damit befassten, das Verhalten von Gehirnzellen vorherzusagen. Ihr Modell hat den Vorteil, dass die Zahl vermuteter Voraussetzungen auf nur eine zentrale Annahme minimiert wurde. *Da*

PC-Sicherheitslücke

Der Rechner wird zur „Quasselstrippe"

Auch ein Rechner kann zur „Quasselstrippe" werden: Sie können sogar miteinander kommunizieren – ohne Netzzugang. Und ohne Befehl des Nutzers. Eine vollständige Isolierung selbst von Computern mit Inhalten höchster Geheimhaltungsstufe ist dadurch massiv erschwert. Sogar streng geheime Daten können ausspioniert werden.

Science Fiction? Spionagethriller? Weder noch, zum Einsatz kommt bewährte Standardtechnologie: Eingebaute Lautsprecher und Mikrofone können Signale von bis zu 20 Kilohertz verarbeiten, manche auch noch höhere Frequenzen. „Nur Menschen mit einem exzellenten Gehör könnten eventuell hochfrequente Signale im Ultraschallbereich wahrnehmen, sie aber kaum als ‚Daten' erkennen", erläutert Prof. Dr. Jörg Keller. Er betreut die externe Promotion von Michael Hanspach an seinem Lehrgebiet Parallelität und VLSI an der FernUniversität in Hagen.

Michael Hanspach (li.) und Prof. Jörg Keller

„Im Rahmen meiner Arbeiten für meine Dissertation – die ich gerade eingereicht habe – konnte ich nachweisen, dass Computer selbstständig über unhörbare Audiosignale versteckte Netzwerke bilden und so heimlich miteinander ‚reden' können", so Michael Hanspach. Seine Erkenntnisse wurden in der Öffentlichkeit bereits stark beachtet.

Die Kommandostruktur eines solchen Spionagenetzwerks ist ganz einfach: Ein Hacker sendet seine Befehle per Internet los, ein – zuvor per USB-Stick, Programm oder Internetanschluss – infizierter Rechner nimmt sie auf und „fragt" in seiner Umgebung akustisch nach, ob es einen „Kollegen" gibt, der ihn versteht (weil er ebenfalls infiziert ist). Meldet sich einer, werden die Befehle an ihn akustisch weitergereicht.

„Beute" wird zurückgeflüstert

Der Hacker kann dann beliebige Befehle über das akustische Netzwerk versenden. Sofern einer der Rechner mit dem Internet verbunden ist, kann er dafür auch dieses verwenden. Die Schadsoftware auf einem infizierten Rechner führt die erhaltenen Anweisungen aus, spioniert private oder geschäftliche Daten aus, verändert sie u.v.m. Die „Beute" wird dann wieder von Maschine zu Maschine „zurückgeflüstert" bis zu der mit Internetzugang. „Auch Tablets und Smartphones können in solche Spionage-Netzwerke einbezogen werden", so Michael Hanspach. Oder die Hacker verschaffen sich Rechenzeit und Speicherplatz.

Die Datenübertragung zwischen infizierten Rechnern erfolgt per Ultraschall. Die Infizierung selbst ist auf diesem Weg jedoch nicht möglich.

Ausgehend von der selbst gestellten Frage, ob die Datenübertragung akustisch übertragen werden könnte, entwickelte Hanspach einen Versuchsaufbau mit fünf handelsüblichen Laptops, von denen nur eins Internetzugang hatte. Damit konnte er beweisen, dass Computer im und knapp unter dem Unterschallbereich Signale in einer Entfernung von bis zu 20 Metern austauschen können.

Hanspach stellte fest, dass infizierte Rechner weitere infiltrierte Geräte in ihrer Nähe ermitteln und mit ihnen ad hoc und nur für diesen Zweck ein „Mesh-Netzwerk" bilden können: „In einem solchen ‚vermischten Netz' werden die Signale über mehrere Stationen weitergeleitet." Störende Geräusche wie lautes Reden wurden von der Schadsoftware herausgefiltert und beeinträchtigten die Datenübertragung nicht, wohl aber Personen, die durch den Versuchsaufbau liefen. Die Rechner müssen zudem direkten „Blickkontakt" haben, reflektierte Signale können nicht verarbeitet werden.

Abhilfe nicht einfach

Die Gegenmaßnahmen sind nur auf den ersten Blick einfach: Lautsprecher und Mikrofon abschalten und ggf. ausbauen oder Softwarefilter implantieren, die verdächtige Signale eliminieren, wenn man Audiodateien abspielen muss. „Wichtig ist daher, zunächst den Handlungsbedarf zu erkennen, bevor man systematisch Schutzmaßnahmen ergreift", betont Hanspach.

Selbst das Ausschalten akustischer Signale kann keine völlige Sicherheit garantieren. Die Tastaturanschläge können ebenso ausgewertet werden wie das Blinken einer LED oder die Frequenz, mit der ein Prozessor arbeitet, erläutert Prof. Keller: „Ein Infrarotsensor kann die Temperaturschwankungen des Prozessors wahrnehmen. Selbst der Stromverbrauch gibt Geheimnisse preis."

Abhilfe könnte ein „Audio Intrusion Detection"-System schaffen, an dem Hanspach arbeitete: „Hiermit können Signale im laufenden Betrieb analysiert und mit bereits bekannten Mustern verglichen werden. Das Ganze ist prinzipiell vergleichbar mit einem ‚Virenscanner', nur eben für physikalische Signale."

Einen infizierten Rechner vom Netz zu trennen hilft jedenfalls nicht. *Da*