Drahtloses Abhören von Bussystemen in der Gebäudeautomatisierung

Andreas Attenberger

FH Kufstein Tirol
Web Communication & Information Systems
Andreas.Attenberger@fh-kufstein.ac.at

Zusammenfassung

Mit der zunehmenden Verbreitung von Bussystemen für Anwendungen in Haushalt und Industrie rücken auch verschiedene Sicherheitsaspekte dieser Systeme in den Fokus der Hersteller und Nutzer. In der Regel existieren keine oder nur sehr gering ausgeprägte Schutzmaßnahmen, um die Buskommunikation vor Angriffen beispielsweise auf die Vertraulichkeit und Integrität der ausgetauschten Nachrichten zu sichern. Gestützt auf vorhergehenden Arbeiten zeigt dieser Artikel einen vereinfachten Aufbau zum Logging von Kommunikationsdaten auf dem proprietären TwinBus-System, welches in diesem Fall in einer Klingelsteuerungsanlage zum Einsatz kommt. Diese Abhörmöglichkeit benötigte bisher den Einsatz von speziell angepassten Hardware-Komponenten mit der Platzierung einer Spule in der Nähe der Busleitungen. In dem hier gezeigten Aufbau wird hingegen ein kommerziell verfügbarer Leitungssucher eingesetzt. Mit einem Line-Kabel, Laptop und Audio-Software können Bustelegramme, die durch Drücken des Klingeltasters verschickt werden, einfach abgehört werden. Dabei kann beobachtet werden, dass sich der Telegramminhalt auch bei mehrfachem Auslösen nicht verändert. Für Umgebungen, in denen vertrauliche Inhalte ausgetauscht werden, beispielsweise in Forschung und Industrie, kann diese Methode der Telegrammaufzeichnung eine potentielle Bedrohung darstellen. Wenn Nachrichten ohne Prüf-Code wiederholt werden können, sind verschiedene Angriffsszenarien beispielsweise mit unbemerkter Datenveränderung oder Identitätsdiebstahl möglich.

1 Einleitung

Feldbussysteme werden seit langem in verschiedenen Industriezweigen beispielsweise der Ansteuerung von Kfz-Steuergeräten [Bosc14] oder dem Betrieb von Produktionsmaschinen eingesetzt werden. Zwischenzeitlich steigt die Verbreitung dieser Kommunikationssysteme weiter, insbesondere vor dem Hintergrund moderner Entwicklungen wie Smart Homes oder dem in Deutschland beworbenen Industrie 4.0 Konzept [VDIE13]. Neben der Verteilung nehmen auch die Kommunikationslast und Zahl der angeschlossenen Knoten weiter zu [Irwi11]. Gleichzeitig wird der Sicherheit dieser Systeme nur wenig Aufmerksamkeit zugeteilt. Große Unternehmen sind sich zwar der Gefahr bewusst, allerdings werden in der Regel vor allem Angriffsszenarien betrachtet, die durch die Verbindung mit externen Netzwerken entstehen können, beispielsweise wenn Fabrikroboter von Rechnern im Internet, welche sich außerhalb der Produktionsstätte befinden, angesteuert werden [Ecke14].

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 388-397.

Dieser Artikel widmet sich hingegen der Möglichkeit neuer Angriffsmöglichkeiten durch das Abhören der Busleitungen zwischen den angeschlossenen Knoten ohne physische Eingriffe. Diese Schwachstelle wurde zuvor schon von Mundt et al. untersucht, welche die Leitungskommunikation ohne physischen Anschluss abhören konnten [MuDG15]. Dabei wurden KNX-Bus-Datentelegramme mit einer Spule, die an der Wand in entsprechender Nähe zu der darunterliegenden Verdrahtung angebracht wurde, abgehört. Die dabei nötige Hardware wurde speziell für diesen Versuch entwickelt und angepasst. In diesem Artikel hingegen wird ein deutlich einfacheres Setup vorgestellt, bei welchem derselbe Effekt mit handelsüblichen, kommerziell verfügbaren Komponenten erzielt wird, was den nötigen Aufwand und entsprechende Hürden für potentielle Angriffe stark herabsenkt.

Beim KNX-System handelt es sich um ein Kommunikationssystem für die Gebäudeautomatisierung. Der Feldbus erlaubt den Austausch verschiedener Informationen von Steuerungsanweisungen für die Gebäudebeleuchtung bis hin zur Sensordatenübertragung beispielsweise von Feuchtigkeits- oder Temperaturdaten. Weiterhin können auch Fenster- und Türkontrolle oder Fingerprintsysteme zur Zugangskontrolle angebunden werden. Ursprünglich als European Installation Bus (EIB) standardisiert ist der KNX-Bus einer der meist verbreiteten Feldbusse in diesem Anwendungsbereich [Knx14]. Ein konkurrierender aber proprietärer Standard ist der RITTO TwinBus, der über eine ähnliche Struktur und ein ähnliches Funktionsprinzip bei einem etwas geringeren Funktionsumfang verfügt [RITT09]. Grundlegende Anwendungsszenarien dieser Feldbusse unterscheiden dabei in der Regel zwischen Sendern und Empfängern [Knx14]. In dem hier betrachteten Anwendungsfall wird ein Türklingelsystem betrachtet, bei welchem sich an der Gebäudeeingangstür ein entsprechendes Klingelschild mit Knöpfen für alle Wohneinheiten befindet.

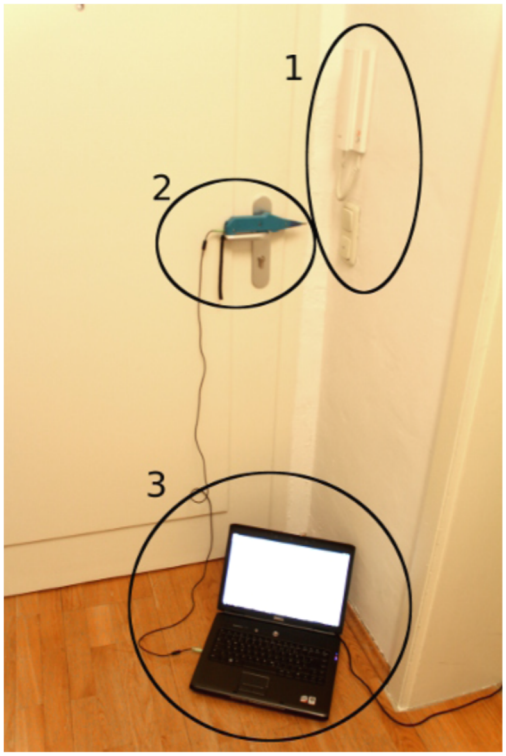

Abb. 1: Aufbau mit (1) Klingelempfänger, (2) Leitungssucher, (3) Laptop mit Audio-Software

2 Methode

Abbildung 1 zeigt den Hardware-Aufbau des zum Abhören der Busnachrichten genutzten Systems. Dabei wurden die Datentelegramme aufgezeichnet, die nach Druck einer Klingel an der Haustüre entsprechend an die Türklingelempfänger in den jeweiligen Wohneinheiten geschickt werden. Ein Leitungssucher von Kurth Electronic ist mit dem Mikrofoneingang eines Laptops verbunden. Auf diesem wird die Open Source Audiobearbeitungssoftware Audacity genutzt, um die akustischen Signale, die vom Leitungssucher ausgegeben werden, aufzunehmen und weiterzuverarbeiten. Das Leitungssuchwerkzeug verfügt über eine entsprechende Taste um den Suchmodus zu aktivieren und entsprechende Leitungssignale empfangen und entweder über den eingebauten Lautsprecher oder über den Klinkenstecker an angeschlossene Geräte auszugeben. Die Tonaufnahmen wurden mit 44,1 kHz und 32-Bit Dynamikumfang aufgenommen während der Leitungssucher aktiviert und eine Klingeltaste am Hauseingang gedrückt wurde. Da der Mikrofoneingang des Laptops genutzt wurde, wird eine entsprechende Mono-Audiospur aufgenommen.

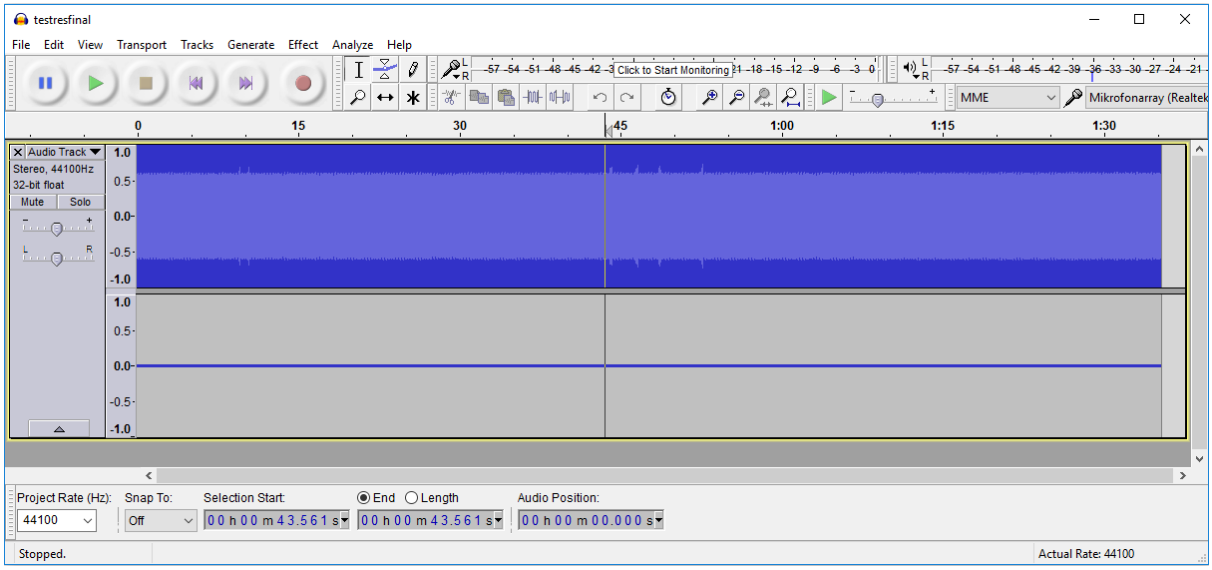

Abb. 2: Aufnahme des vom Leitungssucher ausgegebenen Signals mit der Audacity Audio-Software

Da das aufgenommene Signal sehr starkes Hintergrundrauschen aufweist, welches schon bei Benutzung des im Leitungssucher eingebauten Lautsprechers stark wahrnehmbar ist, muss eine entsprechende, anschließende Signalverarbeitung zur Rauschunterdrückung durchgeführt werden. Unter anderem ist aufgrund der Stromversorgung des TwinBus-Systems über die Netzspannung ein 50 Hz Störsignal enthalten. Abbildung 2 zeigt das aufgenommene Signal vor der weiteren Filterung. In der Mitte der Aufnahme können mehrere Signalspitzen, welche den durch Drücken der Klingeltasten übertragenen Telegrammen entsprechen, identifiziert werden. Eine Verbesserung des Signal-Rausch-Abstandes kann durch Anwendung eines 50-Hz-Kerbfilters erreicht werden. Nach Anwendung dieser grundlegenden Filterungsschritte ist das Nutzsignal besser sichtbar und erlaubt eine erste visuelle Inspektion der übertragenen Daten. Zwar sind die tatsächlichen Signaleigenschaften und Protokollabläufe für den TwinBus nicht öffentlich, allerdings können ähnliche Eigenschaften wie beim KNX-Bussystem angenommen werden. Dabei existieren verschiedene Methoden der Bitübertragung über die Busleitungen, wie in Abbildung 3 gezeigt.

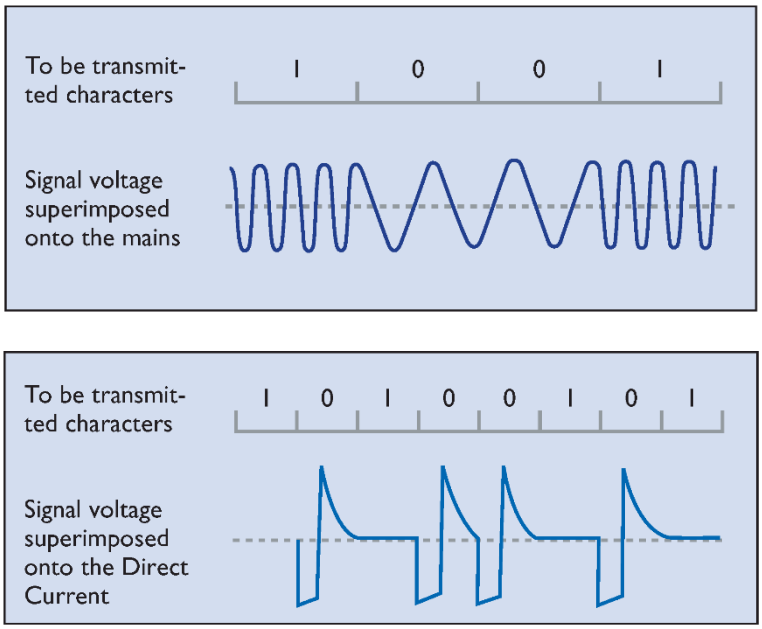

Abb. 3: KNX-Bitübertragung (oben: Frequenzmodulation, unten: Impulse auf Gleichstrom) [Knx14]

Entweder wird ein entsprechender Spannungswert für die High-/Low-Bit-Level über die Leitung übertragen oder die beiden Bit-Zustände werden jeweils von einer unterschiedlichen Frequenz repräsentiert, die auf das DC-Signal der Leitungen aufmoduliert wird. Aufgrund der aufgenommen Signale wird davon ausgegangen, dass es sich im vorliegenden Fall des TwinBuses um die zweite Übertragungsmethode handelt, da zwei unterschiedliche Frequenzen während der Telegrammübertragung im Spektrum sichtbar werden. Nach Tastendruck wird augenscheinlich zuerst eine Startnachricht mit der Frequenz mit 7750 Hz übertragen, welche für einen der beiden Signalzustände steht. Anschließend kommt es zu einer Übertragung mit gelegentlichem Wechsel zwischen 7750 und 15500 Hz Signalen. Dadurch können die übertragenen Daten entsprechend analysiert werden, wie in Abbildung 4 sichtbar.

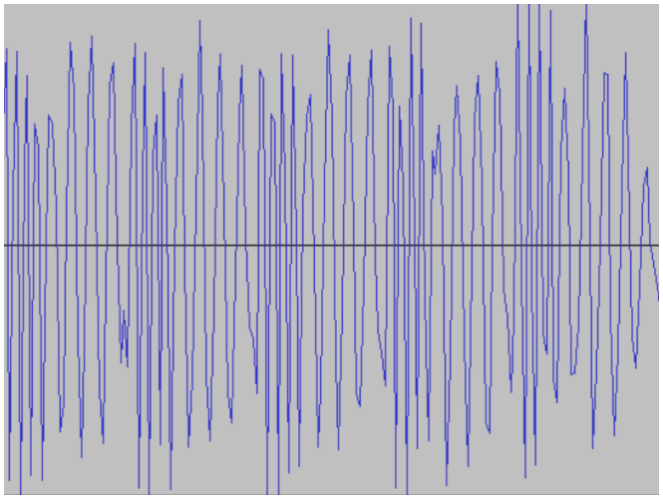

Abb. 4: Nach Rauschfilterung werden die übertragenen Bitmuster sichtbar

3 Datenanalyse

Aus den aufgenommen Daten können verschiedene Rückschlüsse gezogen werden. Im ersten Teil dieses Abschnitts erfolgt eine Bedrohungsanalyse mit Hilfe von verbreiteten IT-Sicherheitsmodellen. Im zweiten Teil werden erste Schritte zu einem Ansatz zur tiefergehenden Protokollanalyse unter Nutzung von Mustererkennungsmethoden aufgezeigt.

3.1 Bedrohungsanalyse

Bereits ohne detaillierte Protokollanalyse können mehrere Schwachstellen des Systems aus dem durchgeführten Experiment abgeleitet werden. Im sogenannten CIA-Triad (Confidentiality, Integrity and Availability) ist beispielsweise die Vertraulichkeit (Confidentiality) dadurch gefährdet, dass die Kommunikationsdaten einfach abgehört werden können. Dies ist besonders dann problematisch, wenn zusätzlich weitere Daten wie Kommunikationsinhalte über den Bus übertragen werden. Beim TwinBus ist dies mit zusätzlichen Adaptern möglich [RITT06]. Dann können nicht nur Knotenadressen – wie in diesem Artikel aufgezeigt – sondern zusätzlich auch Dateninhalte mit dem oben beschriebenen Aufbau mitgeloggt werden. Oft sind die Busleitungen über entsprechend große Distanzen in Gebäuden verteilt. Als Konsequenz können Angreifer aus anderen Gebäudeteilen oder Räumen, die eventuell nicht zu der angegriffenen Institution gehören, die Businhalte entsprechend abgreifen ohne physischen Zugang zur Verkabelung zu benötigen.

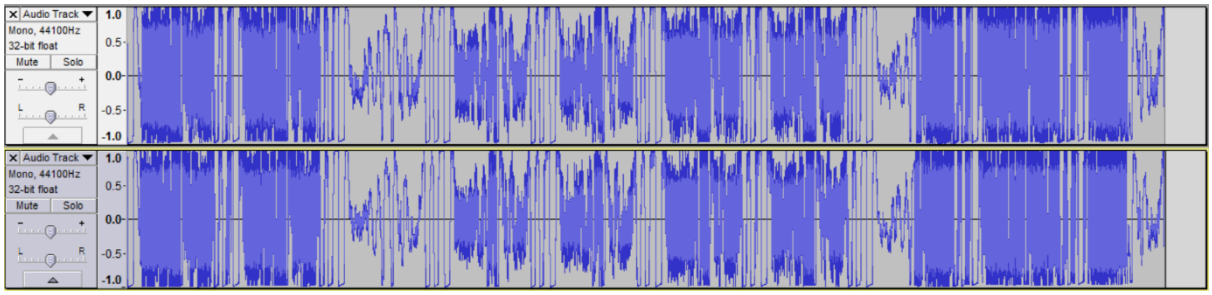

Abb. 5: Aufnahmen der Klingeltelegramme für dieselbe Wohneinheit zu unterschiedlichen Zeitpunkten

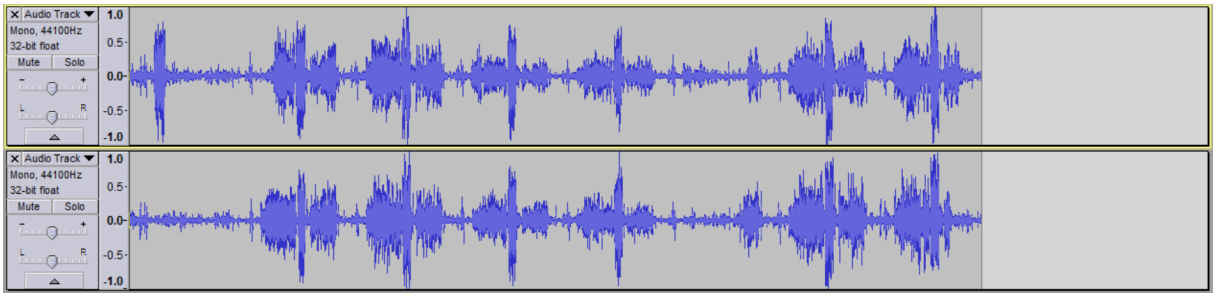

Abb. 6: Klingeltelegramme für verschiedene Wohneinheiten mit teils unterschiedlichem Inhalt

Ohne eine genauere Datenanalyse durchführen zu müssen, ist eine der Haupterkenntnisse des durchgeführten Experimentes, dass beispielsweise dasselbe Telegramm zur Aktivierung eines Türklingelempfängers bei nochmaligen Tastendrücken entsprechend wiederholt wird. Dies ist in Abbildung 5 ersichtlich, welche die beim zweimaligen aufeinanderfolgenden Aktivieren der Klingel gesendeten Daten zeigt. Das übertragene Telegramm unterscheidet sich auch bei einfacher optischer Prüfung von den Daten, die für andere Wohneinheiten übertragen werden, wie

Abbildung 6 mit einem Mitschnitt der Buskommunikation während der Aktivierung der Türklingel zweier verschiedener Wohneinheiten im selben Gebäude zeigt. Damit könnten Informationen über Besuchsfrequenz oder Anwesenheit von Mietern gesammelt werden. Da keine physischen Eingriffe oder Anwesenheit in unmittelbarer Nähe der Gebäudeeinheiten erforderlich sind, können damit auch Strategien des Social Engineering im Bereich der Informationssammlung mit geringeren Hürden ausgeführt werden [Hadn10].

Falls die präsentierte Abhörmethode um die Möglichkeit erweitert wird, auch Daten in den Busverkehr einzubringen, sind Angriffe auf Integrity (Integrität) und Availability (Verfügbarkeit) im CIA-Triad sowie weitere Attacken, wie im STRIDE-Modell [Shos14, MMD+06] denkbar. Das Modell umfasst die in Tabelle 1 aufgestellten Aspekte bei der Kategorisierung von Bedrohungen mit entsprechenden Gegenmaßnahmen.

Tab. 1: Übersicht über Bedrohungen und Gegenmaßnahmen im STRIDE-Modell [MMD+06].

Bedrohung	Gegenmaßnahmen
Spoofing Identity (Fälschen einer Identität)	Authentifizierung Schutz der Passwörter / Secrets Kein Speichern der Passwörter (Secrets)
Tampering with Data (Datenmanipulation)	Autorisierung Hashes Nachrichtenauthentifizierung mit Codes Tamper-Proof-Protokolle
Repudiation (Ablehnung der Verantwortlichkeit)	Digitale Signaturen Zeitstempel Auditierungspfade
Information disclosure (Preisgabe von Informationen)	Autorisierung Privacy-enhanced Protokolle Verschlüsselung Schutz der Passwörter (Secrets) Kein Speichern der Passwörter (Secrets)
Denial of Service (Dienstverweigerung)	Filterung Reduktion des Dienstgüte
Elevation of Privilege (Berechtigungserweiterung)	Ausführung nur mit notwendigen Rechten

Bei der Analyse des vorliegenden TwinBus-Systems wird deutlich, dass im STRIDE-Modell mehrere Bedrohungsfälle zutreffen für die keine der angegebenen Gegenmaßnahmen implementiert wurden. Beispielsweise scheint kein Mechanismus zur Verhinderung von duplizierten Telegrammen vorhanden zu sein. Dadurch wären auch Angriffe auf Dateninhalte wie Identity Spoofing möglich. Ebenfalls könnten die Payloads von Telegrammen manipuliert werden (Tampering with Data), da augenscheinlich kein Hashing oder andere Arten von Nachrichtenauthentifizierung beziehungsweise andere Autorisierungsarten in Verwendung sind. Dadurch sind weiterhin Repudiation-Attacken möglich, bei denen Nutzer behaupte, eine entsprechende Handlung nicht ausgeführt zu haben. Nachdem der Adressat eines Telegramms auf einfache Weise festgestellt werden kann, ist auch die Preisgabe von Informationen eine der möglichen

Bedrohungstypen wenn Bussysteme insbesondere zur Übertragung von weiteren Informationen neben den vorliegenden Adresstelegrammen genutzt werden. Weiterhin kann auch die Verfügbarkeit des Bussystems entsprechend gestört werden, beispielsweise durch Injizieren einer Vielzahl fehlerhafter Nachrichten oder die Überlastung von Aktuatoren oder Empfängern mit dem Resultat eines Denial of Service. Eine Rechteverwaltung ist auf Busknotenebene denkbar, durch die aktuelle offene, unverschlüsselte Überschlüsselung aber ohne zusätzlichen Nutzen. Die Gefahr der Berechtigungserweiterung besteht bei den betrachteten Systemen nicht auf Kommunikationsseite sondern in der Realisierung der Busknotenfunktionalität, welche nicht Teil der Betrachtung ist.

Neben den Elementen der CIA- und STRIDE-Modelle wurden darüber hinaus in einer vergangenen Untersuchung auch Gefahren für die Privatsphäre von Nutzern durch langanhaltendes Nachrichten-Logging festgestellt [MuDG15].

3.2 Protokolldatenanalyse

Eine der derzeitigen Beschränkungen des demonstrierten Aufbaus ist das Fehlen einer Signalanalyse auf Protokoll-Level. Dieses Problem wird zusätzlich durch das verwendete, proprietäre TwinBus-Protokoll weiter verschärft. Wie in den Abbildungen 5 und 6 erkennbar lässt die Signalqualität keine eindeutige, direkte Zuordnung von Signalteilen zur Bit-Level-Übertragung zu. Langfristiges Loggen von Busnachrichten – beispielsweise in Kombination mit maschineller Musterkennung – wäre dabei allerdings eine Möglichkeit, um das verwendete Protokoll im Detail weiter zu analysieren. Bei der Verwendung von offenen Standards würde dieser Faktor allerdings wegfallen.

Eine Möglichkeit, der Situation von proprietären Standards zu begegnen, ist der Einsatz von Techniken des maschinellen Lernens [DuHS01]. Dabei werden die aufgenommenen Quelldaten – hier die unterschiedlichen Telegrammaufzeichnungen – wie in Abbildung 7 dargestellt beim Labelling und Segmentieren getrennt und jeweils einer Klasse, beispielsweise Wohneinheit 1 oder Wohneinheit 2, zugeordnet. Anschließend erfolgt die Merkmalsextraktion bei der aus den ursprünglichen Rohdaten mit bestimmten Merkmalsberechnungsmethoden entsprechend charakteristische Datenpunkte extrahiert werden. Anschließend werden die Merkmalswerte genutzt, um ein Klassifizierermodell zu trainieren. Dabei kann auf eine Vielzahl verschiedener Methoden des maschinellen Lernens zurückgegriffen werden. Diese umfassen unter anderem Entscheidungsbäume, Neuronale Netze oder Support Vektor Maschinen (SVM).

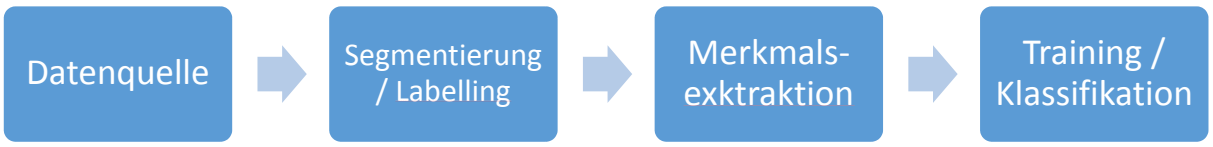

Abb. 7: Der grundlegende Klassifikationsprozess.

Eine Möglichkeit der Feature- beziehungsweise Merkmalsberechnung ist die Extraktion des durchschnittlichen Betrages (Mean Absolute Value) der aufgezeichneten Sample-Werte während der Übertragung eines Telegrammes. Dabei wird in einem festgelegten Zeitfenster von beispielsweise 128 Samples zuerst der Betrag aller Datenpunkte und anschließend deren Durchschnittswert bestimmt. Für eine Fenstergröße von N Samples wird der Mean Absolute Value (MAV) dann wie folgt berechnet:

$$MAV = \frac{1}{N}\sum_{k=1}^{N}|x_k|$$

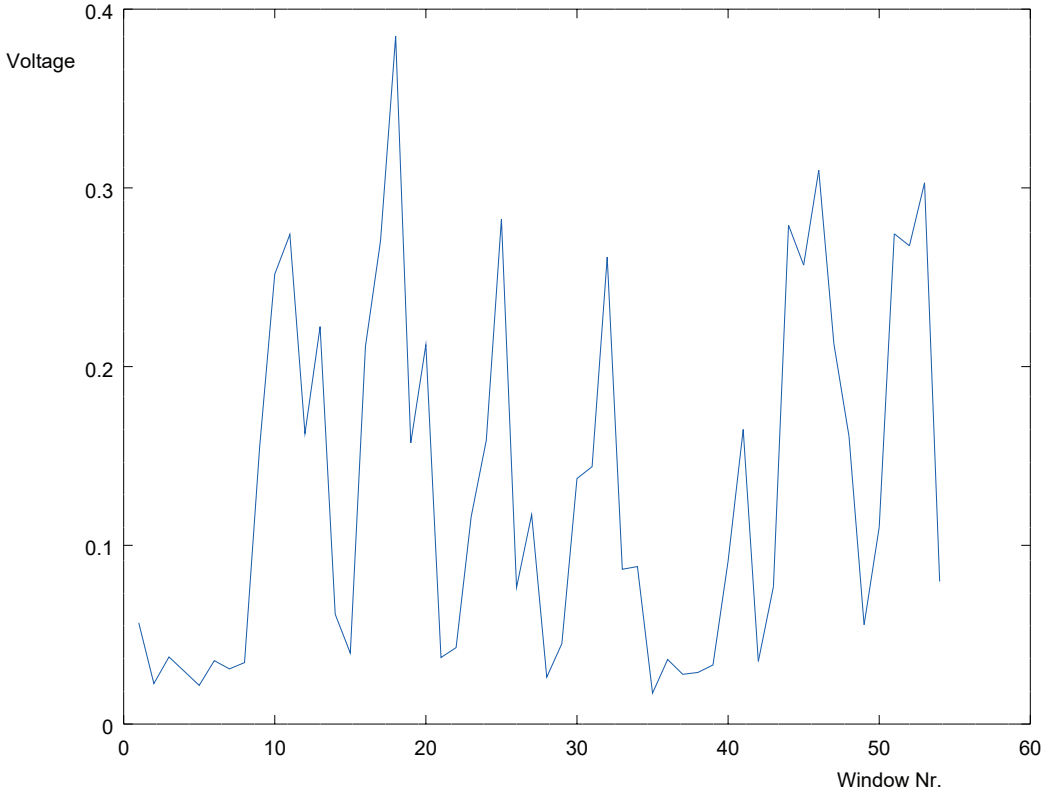

Abb. 8: Aus den Rohdaten (Abbildung 6 unten) extrahierte MAV-Merkmalswerte.

Abbildung 8 zeigt die Berechnung der MAV-Werte mit einer Fenstergröße von 128 ohne Überlappung der Fenster bei einer ursprünglichen Sampling-Frequenz von 44,1KHz für das in Abbildung 6 unten dargestellte Datentelegramm der zweiten Wohneinheit. Zur Berechnung wurden die aufgenommen Audiodaten mit Audacity in das Microsoft PCM Wav-Format exportiert. Anschließend wurden die Beträge der Sample-Werte und Durchschnittswerte pro Fenster mit GNU Octave 4.0.3 berechnet.

Ob der MAV-Wert ein sinnvolles Merkmal für die Detektion von unterschiedlichen Datentelegrammen ist, muss zuerst durch entsprechende Testreihen geklärt werden. Dabei kann beispielsweise mit unterschiedlichen Merkmalsmethoden geprüft werden, wie hoch für existierende Testdaten mit bekannter Klassenzugehörigkeit die Erkennungswahrscheinlichkeit bei der Klassifizierung ausfällt. Mögliche Alternativen zur MAV-Extraktion wäre die Nutzung von frequenzbasierten Merkmalen wie der durchschnittlichen Frequenz oder die Wellenlänge. Ebenfalls können komplexere Methoden wie die Wavelet Transformation genutzt werden

[ThKo08]. Die Erkennungswahrscheinlichkeit kann auch von der Wahl des Klassifizierers abhängen, weshalb hier eine entsprechende Auswahl getroffen werden muss. Da dieser Zusammenhang aber nicht so stark ausgeprägt ist [DuHS01], kann diese Entscheidung nach abgeschlossener Auswahl passender Merkmale in weiteren Testschritten erfolgen. In jedem Fall ist eine größere als die in dieser Arbeit aktuell vorliegende Datenbasis notwendig, um die jeweiligen Methoden zu selektieren und zu validieren.

Weiterhin ist derzeit unklar, wer oder was potentielle Angriffsziele sein könnten. Zumindest sind besonders solche Institutionen oder Personen gefährdet, die diese Systeme in größeren Gebäuden einsetzen, bei denen gemeinsame Busleitungen auch über weitere Strecken oder durch Nachbargebäude verlaufen.

4 Zusammenfassung und Ausblick

Dieser Artikel demonstriert eine einfache Methode zum Abhören von Gebäudeautomatisierungssystemen, welche eingesetzt werden, um verschiedene Informationen von kritischen Infrastrukturkontrolldaten bis hin zu Kommunikationsinhalten zu übertragen. Mit frei verfügbaren Hilfsmitteln und ohne spezielles technisches Wissen, ist es möglich, Bustelegramme aufzunehmen und grundlegende Datenanalysen wie das Erkennen von gleichen Bitmustern auszuführen. Ebenfalls möglich ist die Zuordnung von Telegrammen zu einzelnen Busteilnehmern. Damit können Informationen über Wohn- oder Geschäftsparteien in Gebäuden gewonnen werden, beispielsweise um Angriffe im Bereich des Social Engineering vorzubereiten. Eine genauere Analyse könnte tiefergehende Erkenntnisse über die übertragenen Daten mit entsprechenden Angriffsmöglichkeiten erlauben. Diese umfassen unter anderem Attacken im Sinne des CIA-Triads sowie weitere darüberhinausgehende Szenarien. Neben der Definition dieser Angriffsszenarien sollte in zukünftigen Arbeiten beispielsweise die Möglichkeit der automatischen Protokollanalyse betrachtet werden. In diesem Artikel wird grundlegende Vorarbeit geleistet, um dabei in Zukunft auch Mustererkennungsmethoden zur Telegrammbestimmung einsetzen zu können. Dafür wurde in diesem Artikel das grundlegende Vorgehen beispielsweise für die Merkmalsextraktion demonstriert. Weiterhin sollte durch umfassendes Logging eine Datenbasis geschaffen werden, um Merkmalsberechnung und maschinelle Lernalgorithmen auf den anfallenden Daten zu testen.

Literatur

[Bosc14] Robert Bosch GmbH: Bosch Automotive Electrics and Automotive Electronics: Systems and Components, Networking and Hybrid Drive, Springer Vieweg (2014).

[DuHS01] R. Duda, P. Hart, D. Stork. Pattern Classification. Wiley (2001).

[Ecke14] C. Eckert: IT-Sicherheit und Industrie 4.0. In: Mio Magazin für Innovation, Organisation und Management, Special 01/2014 (2014) 40-45.

[Hadn10] C. Hadnagy: Social Engineering: The Art of Human Hacking, John Wiley & sons (2010).

[Irwi11] J. D. Irwin: Industrial communication systems. CRC Press (2011).

[Knx14] www.knx.org: The KNX Standard - The Basics (2014).

[MMD+06] J.D. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, A. Murukan: Improving Web Application Security: Threats and Countermeasures. Microsoft Corporation (2006).

[MuDG15] T. Mundt, A. Dähn, H.-W. Glock: Forensic analysis of home automation systems. In: Datensicherheit und Datenschutz 510 (2015) 190-197.

[RITT06] RITTO: Ritto TwinBus Wohntelefon DECT Art.-Nr. 1 7680 Bedienungsanleitung (2006).

[RITT09] RITTO: Ritto TwinBus-KNX-Umsetzer Art.-Nr. 1 7763 (2009).

[Shos14] A. Shostack: Threat modeling: Designing for security. John Wiley & Sons (2014).

[ThKo08] S. Theodoridis, K. Koutroumbas. Pattern Recognition, fourth edition, Academic Press (2008).

[VDIE13] Verein Deutscher Ingenieure e.V., VDI/VDE Gesellschaft Mess- und Automatisierungstechnik (GMA): Thesen und Handlungsfelder, Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation (2013).