Security-Monitoring beim Pairing in Wireless Sensor Networks

Ina Schiering[1] · Arne Hitzmann[2]
Oliver Krebs[1] · Tom Lorenz[1]

Ostfalia HaW[1]
Institut für Information Engineering
{i.schiering | oli.krebs | tom.lorenz1}@ostfalia.de

Osaka University[2]
Graduate School of Engineering Science
arne.hitzmann@arl.sys.es.osaka-u.ac.jp

Zusammenfassung

Der Trend der Digitalisierung basiert auf der Technologie des Internet of Things. Ein wichtiges Element des Internets of Things sind Wireless Sensor Networks. Dabei werden eine Reihe von Sensoren oder anderen Geräten vernetzt durch Mesh-Netzwerke über ein Gateway mit Back-End Services im Internet verbunden. Diese Geräte haben Einschränkungen bzgl. der Rechenleistung und des Stromverbrauchs, weshalb oft nur eingeschränkt kryptographische Verfahren und Zertifikate eingesetzt werden können. Innerhalb dieses Bereichs werden mögliche Angriffe untersucht und Gegenmaßnahmen entwickelt. Der Fokus liegt dabei auf der Pairing-Phase von Wireless Sensor Networks. In diesem Kontext werden proaktive Maßnahmen entwickelt, um Angriffe zu erkennen und soweit möglich zu erkennen, ob ein Angreifer versucht Teilnehmer des Netzwerks zu werden.

1 Einleitung

Der aktuelle Trend der Digitalisierung hat zu Innovationen in vielen Bereichen, wie Stromnetzen, der Infrastruktur in Städten, Häusern und Produktionssystemen, geführt. Im Zentrum stehen dabei die Techologien des Internet of Things (IoT) und Anwendungen wie Smart Grid, Smart City, Smart Home, E-Health und Industrie 4.0. Dieser Trend wird unterstützt durch den technologischen Fortschritt bei Embedded Devices, Wireless Networks, Virtualisierung und Cloud Computing.

Gubbi et al. [GBMP13] stellt als Ziel des IoT heraus “to make a computer sense information without the aid of human intervention”. In diesem Beitrag werden die zugehörigen Wireless Sensor Networks (WSN) untersucht, die wichtige Elemente in den dargestellten Anwendungsbereichen sind.

WSNs bestehen aus einer Menge von Devices mit begrenzter Rechenleistung und geringem Stromverbrauch, die in ein Mesh-Netzwerk integriert sind. Ein Gateway innerhalb des Netzwerks sammelt Daten und sendet sie nach einer Vorverarbeitung in ein Back-End, bzw. zu einem Cloud Service (Abbildung 1).

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 114-125.

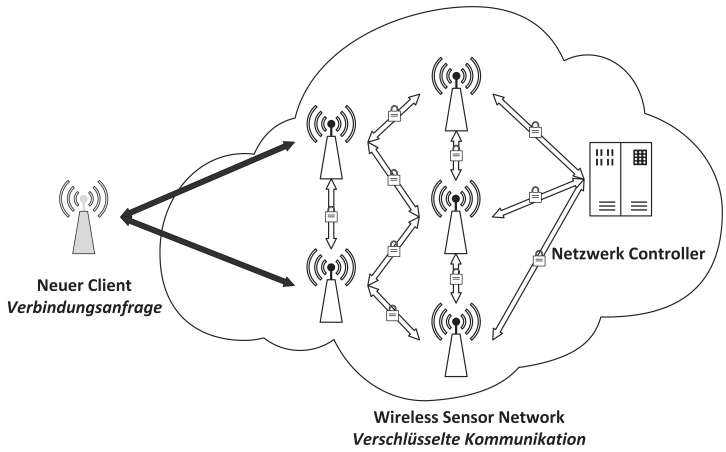

Abb. 1: Kommunikation in WSN

Besonders Geräte für den privaten Bereich müssen preiswert und benutzerfreundlich gestaltet sein. Die meisten der Geräte sind batteriebetrieben und über mobile Netzwerke angebunden. Sensoren müssen dabei kostengünstig, klein und energieeffizient sein, um breit eingesetzt werden zu können. Ein typisches Device verwendet z.B. einen Microcontroller mit einer Taktfrequenz von 7 MHz, 4 kB RAM, 128 kB ROM und 512 kB Speicher [BPCC+07].

Diese technischen Begrenzungen und die Anforderung der einfachen Nutzung im Feld haben zur Einführung von leichtgewichtigen Protokollen, wie Z-Wave, ZigBee, etc. geführt. Zur Interaktion mit Nutzern existiert häufig lediglich eine Status-LED und wenige Tasten. Die Protokolle der WSNs besitzen Funktionen zur autonomen Fehlerbehandlung, so dass Nutzer möglichst nicht mit technischen Details konfrontiert und eventuell überfordert werden.

Im vorliegenden Beitrag werden Angriffe auf WSNs und Ansätze zur Erkennung von Angriffen untersucht. Der Fokus dabei liegt auf der Pairing-Phase von WSNs. Dazu werden effiziente Ansätze vorgestellt, Angriffe durch Monitoring zu erkennen und damit Risiken in WSNs effizient zu minimieren.

Dazu werden zunächst in Abschnitt 2 Technologien für WSNs und aktuell verwendete Sicherheitsmaßnahmen vorgestellt. Anschließend werden in abschnitt 3 Beispiele für Angriffe und Folgen in WSNs erläutert. Bisherige Ansätze für Sicherheitsmaßnahmen (Related Work) folgen in Abschnitt 4. Mit Fokus auf die Pairing-Phase werden Angriffsmuster detailliert in abschnitt 5 analysiert und in Abschnitt 6 Maßnahmen zur Erkennung dieser Angriffe vorgestellt und diskutiert.

2 Security in Wireless Sensor Networks

Die wichtigsten Standards für WSNs im Bereich IoT sind Zigbee und Z-Wave. Wichtig für die hier vorliegende Untersuchung ist die Frage, wie kryptographische Verfahren und Ansätze zur Fehlertoleranz in diesen Protokollen genutzt werden.

ZigBee [ZiSt15] [BPCC+07] [VHPARS+13] erlaubt es, Profile für verschiedene Anwendungen zu definieren. Um Interoperabilität zu gewährleisten und als Fall-Back-Konzept existiert ein Master Key, der Teil des Standards ist, und damit Ansätze für Angriffe bietet.

Der Z-Wave Standard fordert nicht verbindlich die Nutzung von kryptographischen Verfahren

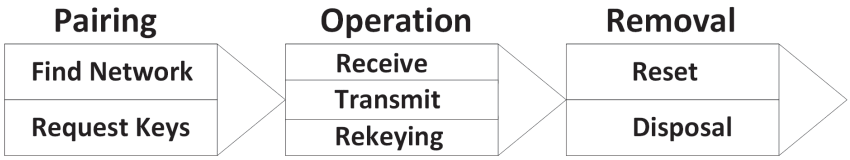

Abb. 2: Phasen im Life-Cycle eines WSN Device

bei der Zertifizierung von Geräten. Hall und Ramsey [HaRa16] stellen dar, dass von 33 untersuchten Z-Wave Geräten lediglich 9 kryptographische Verfahren unterstützen. Fouladi and Ghanoun [ZlGh13] betrachten die optionale Verschlüsselung in Z-Wave als sicher. Fuller und Ramsey [FuRa15] stellen dar, wie Angreifer neue Geräte zum Netzwerk hinzufügen können.

Derzeit werden bei WSNs meist symmetrische kryptographische Verfahren (*AES-128 CCM*) eingesetzt [HZLH09], die effizient in diesem Umfeld genutzt werden können und auch bei ZigBee und Z-Wave Verwendung finden [ZiSt15, ZlGh13]. Der Einsatz von asymmetrischen Verfahren würde die Notwendigkeit von systemweiten Master-Keys vermeiden und wäre auch realisierbar nach [LMKG+09], wird aber derzeit nicht umgesetzt.

Die Hauptursache für erfolgreiche Angriffe in WSNs sind derzeit die Rahmenbedingungen der Devices und der zugehörigen Netzwerke. Die Geräte müssen preiswert sein, energieeffizient arbeiten und leicht zu verwenden sein. Fehler im Betrieb müssen behandelt werden, ohne das Benutzer eingreifen müssen, um die einfache Nutzung zu gewährleisten. Neben Angriffen auf die Implementierung von kryptographischen Verfahren, reicht es oft schon als Angreifer ein Verhalten zu zeigen, mit dem die Entwickler nicht gerechnet haben, um selber Devices ins Netzwerk einzuschleusen [HaRa16, ZlGh13].

Ist ein Angreifer erst Bestandteil des Netzwerks, ist er in der Lage zum Beispiel Daten zu lesen und zu verändern oder das Routing zu manipulieren, um Man-in-the-Middle-Attacken zu ermöglichen [FrTA13].

3 Angriffe auf Wireless Sensor Networks

Der Life-Cycle eines typischen WSN Devices besteht aus den folgenden Phasen, die auch von einem Angreifer durchlaufen werden müssen, um Bestandteil des Netzwerks zu werden und dabei das Verhalten eines legitimen Clients zu imitieren. Zunächst muss ein neues Gerät durch *Pairing* Bestandteil des Netzwerks werden. Nach der Betriebs-Phase (*Operation*) wird das Gerät potentiell wieder aus dem Netzwerk entfernt (*Removal*). Diese Phasen werden in Abbildung 2 dargestellt.

Aufgrund der Bedeutung von WSNs sind Devices und Netzwerke häufig Ziele von Angriffen [PeSW04]. Die hier dargestellten Angriffe werden in Tabelle 1 zusammengefasst. Einen Überblick über Methoden für Angriffe auf WSNs stellen Sharam und Ghose [ShGh10] dar. Manipulation der Hardware, das sogenannte *Hardware Tampering* kann eingesetzt werden, um Informationen aus dem Speicher oder über Wartungs-Interfaces auszulesen. Bei der *Exhaustion Attack* wird durch energieintensive Interaktion versucht, die Batterie eines Devices zu leeren.

Weitere Angriffe auf WSNs konzentrieren sich im Wesentlichen auf die Manipulation des Netzwerks. Um die Kommunikation im gesamten Netzwerk zu unterbinden, wird in [LHDH+05] der Ansatz des *Jamming* vorgestellt, bei dem das Netzwerk durch eine Vielzahl von Nachrichten ge-

zielt überlastet wird. Als Variante kann auch durch *Selective Jamming* die Kommunikation zu einem Device gezielt unterbunden werden [WMSL11].

Angreifer können weiterhin gezielt das Routing im Netzwerk manipulieren. Beim *Sybil-Angriff* versucht ein Angreifer gezielt, indem er gezielt Devices imitiert, Netzwerk-Kommunikation über eigene Geräte zu routen oder durch fehlerhaftes Routing Kommunikation zu verhindern. Ein sogenannter *Wormhole-Angriff* bietet Clients eine effizientere Route zum Netzwerk an, um die versendeten Daten zu analysieren. Mittels dieses Angriffs können auch Geräte an einen anderen Ort bewegt werden, ohne dass sie die Verbindung zum Netzwerk verlieren. Bei einem *Sinkhole-Angriff* bietet sich der Angreifer als effizienter erster Hop im Netzwerk an.

Beim *Evil-Twin*-Angriff und *Spoofing* [BaGM08] versucht der Angreifer Zugang zum Netzwerk zu gewinnen. Dieses sind Angriffe in der Pairing-Phase. Sie werden in Abschnitt 5 detailliert dargestellt und es werden anschließend Maßnahmen zur Erkennung dieser Angriffe untersucht.

Tab. 1: Angriffe auf WSNs und Phasen des Life-Cycle

Angriff	Ziel	Phase des Life-Cycle
Tampering	Informationen erlangen	Operation & Removal
Exhaustion	Lebensdauer der Batterie reduzieren	Operation
Jamming	Netzwerk unterbrechen	Pairing & Operation
Selective Jamming	Kommunikation gezielt unterbinden	Pairing & Operation
Wormhole	Routing manipulieren	Pairing & Operation
Sinkhole	Routing manipulieren	Pairing & Operation
Sybil	Routing manipulieren	Pairing & Operation
Evil Twin	Zugang zum Netzwerk gewinnen	Pairing
Spoofing	unbemerkt Zugang zum Netzwerk gewinnen	Pairing

4 Related Work

Die bisherigen Ansätze bei der Betrachtung von Security in WSN können grob in zwei Gruppen gegliedert werden. Zum einen geht es darum, die Auswirkungen eines Angriffs zu reduzieren, bei dem ein Angreifer in das Netzwerk eindringt [ShGh10], indem Ansätze zum fehlertoleranten Routing betrachtet werden. Zum anderen geht es darum, das Risiko zu bewerten, bei dem ein Knoten des Netzwerks von einem Angreifer kontrolliert wird. Ansätze zum fehlertoleranten Routing werden breit untersucht, siehe Deng et al. [DeHM06], Zhou et al. [ZLCS08], Karlof et al. [KaLP03], Li et al. [LiZL06], Parno et al. [PLGP06], Yao und Zheng [YaZh08], Devisri und Balasubramaniam [DeBa13]. Dabei steht im Vordergrund, dass das Netzwerk-Routing trotz der Präsenz von Angreifern im Netzwerk weiter stabil bleibt.

Um das Eindringen von Angreifern ins Netzwerk zu erkennen, haben Singh et al. [SKKM15] Ansätze der visuellen Kryptographie untersucht, um Teilnehmer im Netzwerk zu validieren. Asokan et al. [ABIS+15] haben die Methode der Device Attestation vorgeschlagen, um große Mengen von Devices effizient zu beurteilen.

Ošťádal et al. [OsSM15] und Jiang and Zhao [JiZh07] arbeiten mit einem zusätzlichen Protokoll, um Vertraulichkeit in einem kompromittierten Netzwerk zu gewährleisten.

Die bisher untersuchten Strategien zur Risikominimierung haben den Fokus im Wesentlichen auf der Operation-Phase. Die Pairing-Phase wurde dabei bisher nicht betrachtet. Deshalb liegt der Fokus des vorliegenden Beitrags auf der Untersuchung von Ansätzen in der Pairing-Phase.

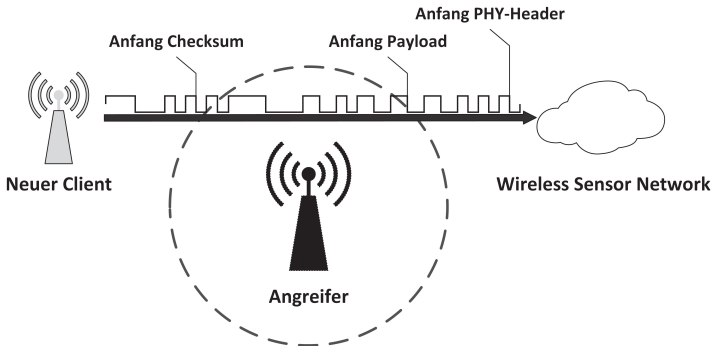

Abb. 3: Ein Angreifer erhält Zugang zum Netzwerk durch Selective Jamming

5 Angriffe in der Pairing-Phase

Die Pairing-Phase ist eine interessante Phase für Angreifer im Lebenszyklus von WSNs, weil Angreifer in dieser Phase Zugang zum Netzwerk erhalten können, ohne Lücken in kryptographischen Verfahren ausnutzen zu müssen [BPCC+07]. Bei der Auswahl der im folgenden dargestellten Angriffe steht im Vordergrund, dass sie von Angreifern unbemerkt ausgeführt werden können. Die Anwendbarkeit der Angriffe ist abhängig von den verwendeten Protokollen. ZigBee und Z-Wave werden aufgrund ihrer Verbreitung als Beispiele verwendet. In Tabelle 2 werden die hier präsentierten Angriffe mit Gegenmaßnahmen zusammengefasst.

Tab. 2: Angriffe in der Pairing-Phase von WSNs

Angriff	Erkennbarkeit	Gegenmaßnahmen
Jamming	nein	Spread Spectrum Techniken
Selective Jamming	begrenzt	Spread Spectrum Techniken
Evil Twin	begrenzt	Pre-Shared Keys
Spoofing	nein	Pre-Shared Keys

5.1 Jamming

Das Ziel des Jamming ist es, Kommunikation in Wireless Networks zu verhindern. In der Pairing-Phase kann dadurch zusätzlich verhindert werden, dass ein neues Device Bestandteil des Netzwerks als Client wird. Interferenzen, ausgelöst z.B. durch Hintergrundrauschen, können wie bereits in mehreren Standards umgesetzt, durch Techniken wie *Direct Sequence Spread Spectrum (DSSS)* [PeZB95] reduziert werden.

Obwohl DSSS generell einen effektiven Ansatz darstellt, wird von Farahani [Fara08] ein Ansatz vorgestellt, der trotzdem Jamming ermöglicht. Weitergehende Ansätze, die Kommunikation über mehrere Kanäle verteilen, wurden von Hang et al. [HaZJ06] beschrieben. Hier muss der Angreifer das Störsignal auf dem richtigen Kanal übertragen. Law et al. [LHDH+05] beschreiben einen Ansatz, trotz DSSS energieeffizient Kommunikation in einem Wireless Network zu stören.

5.2 Selective Jamming

Durch das sogenannte Selective Jamming kann gezielt die Kommunikation zwischen spezifischen Devices gestört werden. Dazu muss der Angreifer die Header der Pakete auswerten.

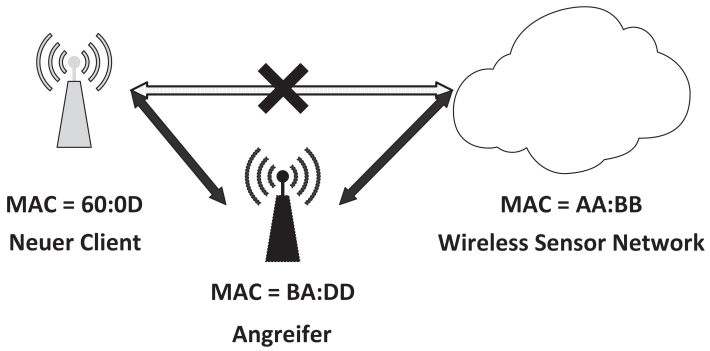

Abb. 4: Evil-Twin-Angriff durch Selective Jamming

Wenn die Quell- und Zieladresse die Verbindung darstellen, die gestört werden soll, sendet der Angreifer gezielt Störsignale (Abbildung 3). Dadurch kann unter anderem die Einbindung in das WSN in der Pairing-Phase gestört werden.

Aufgrund des einfachen und kostengünstigen Designs von typischen WSN Geräten wie z.B. Sensoren, sind die Gegenmaßnahmen gegen Jamming und Selective Jamming begrenzt. Mpitziopoulos et al. [MGKP09] stellen heraus, dass die Nutzung von DSSS in ZigBee solche Angriffe nicht vermeiden kann. Ob Jamming in WSNs immer noch möglich ist, haben Wilhelm et al. [WMSL11] durch eine Evaluation bestätigt.

Der Ansatz des Selective Jamming ist eine wichtige Voraussetzung für die weiteren Angriffstypen, da man dadurch gezielt das erfolgreiche Pairing eines neuen Devices unterbinden kann. Alternativ kann der Angreifer selber Zugang erhalten. Dazu muss der Angreifer zwischen den Devices positioniert sein, deren Kommunikation gezielt gestört werden soll.

5.3 Evil-Twin-Angriff

Das Ziel des Evil-Twin-Angriffs ist es, durch einen Man-in-the-Middle-Angriff Zugang als Client zum Netzwerk zu erhalten, statt eines legitimen neuen Device. Das Device des Angreifers ermöglicht dem legitimen Device den Zugriff auf das eigene, falsche WSN (Abbildung 4). Der Angreifer kann Sensordaten des legitimen Devices lesen und hat die Möglichkeit, dem WSN einen manipulierten Strom von Sensordaten zu übermitteln. Das legitime Device wird erfolgreich Bestandteil des Netzwerks des Angreifers. Dieser Angriff ist eine Variante des von Bauer et al. [BaGM08] vorgestellten Evil-Twin-Angriffs auf WLAN Netzwerke durch die Nutzung von gefälschten WLAN Access Points.

Dadurch, dass der Angreifer seine eigene MAC-Adresse während des Angriffs verwendet, erhält das WSN des Adressaten des Angriffs keine Pakete mit ungültigem Schlüssel [Alli10].

Der Angreifer muss sein Device im Umfeld des eigentlichen Device und des ursprünglichen WSNs belassen, um die Brücke zwischen den beiden aufrecht zu erhalten. Wird das Device des Angreifers entfernt, verliert das legitime Device die Verbindung, da es für das ursprüngliche Netzwerk keine Schlüssel besitzt. Dadurch kann es potentiell zu Fehlermeldungen und Alarmen kommen.

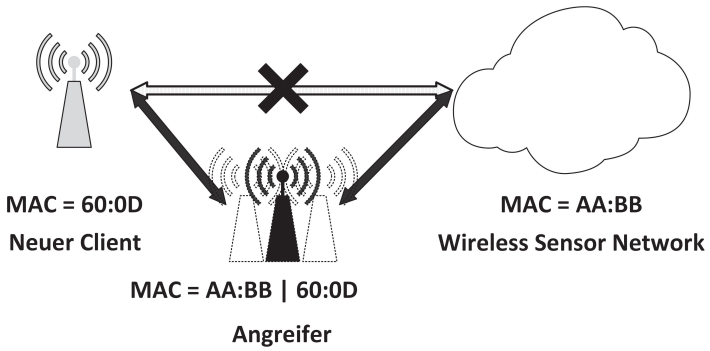

Abb. 5: Spoofing-Angriff als Erweiterung des Evil-Twin-Angriffs

5.4 Spoofing-Angriff

Beim Evil-Twin-Angriff verwendet der Angreifer sowohl gegenüber dem WSN, als auch gegenüber dem legitimen neuen Device dieselbe MAC-Adresse. Als Erweiterung dieses Angriffs kann die MAC-Adresse des neuen Device ausgelesen werden und das Gerät des Angreifers kann sich mit dem WSN mit dieser Adresse verbinden und damit den Angriff verbergen. Dieser Angriff wird als Spoofing-Angriff bezeichnet. Durch die Nutzung der MAC-Adresse des legitimen Device ist der Angreifer für das WSN nicht vom legitimen Device unterscheidbar (Abbildung 5).

Das einzige wahrnehmbare Merkmal dieses Angriffs ist, dass das neue Device und das WSN Pakete mit bekannter Quelladresse und ungültigem Schlüssel empfangen. Dieses Merkmal wird im Folgenden verwendet, um diesen Angriff im Rahmen eines Monitorings zu erkennen.

6 Monitoring zur Erkennung von Angriffen

Das Ziel der hier vorgestellten Konzepte ist es, die Sicherheit in WSNs zu erhöhen, indem das Verhalten von Angreifern in der Netzwerk-Kommunikation erkannt wird. Dazu werden für den Evil-Twin-Angriff und den Spoofing-Angriff in der Pairing-Phase von WSNs Monitoring-Ansätze vorgestellt. Wichtiges Ziel bei den vorgestellten Ansätzen ist, dass keine zusätzlichen Devices und auch keine höhere Performance der Devices benötigt wird.

Die beiden betrachteten Angriffe setzen in der Pairing-Phase eines neuen Device im Netzwerk an. Die zentrale Idee zur Erkennung dieser Angriffe ist, dass Clients des WSNs während des Pairings neuer Devices Netzwerk-Aktivität monitoren. Versucht ein Angreifer die MAC-Adresse eines Device zu duplizieren, kann ein anderer Client im Netzwerk dies erkennen und es an den Netzwerk-Controller melden. Das Monitoring von Netzwerk-Aktivitäten durch Clients verursacht einen erhöhten Energieverbrauch. Deshalb sollte es einen expliziten Pairing-Modus im Netzwerk geben und das Monitoring sollte von bestehenden Netzwerkknoten lediglich während dieser Phase durchgeführt werden.

6.1 Erkennen eines Evil-Twin-Angriffs

Das Ziel bei der Erkennung eines Evil-Twin-Angriffs ist es zu erkennen, dass ein Device als *Bridge* fungiert. Ein Device besitzt zwei generelle Zustände: Zunächst ist es isoliert bevor es mit dem Pairing Bestandteil eines WSN geworden ist. Anschließend ist es ein Client eines

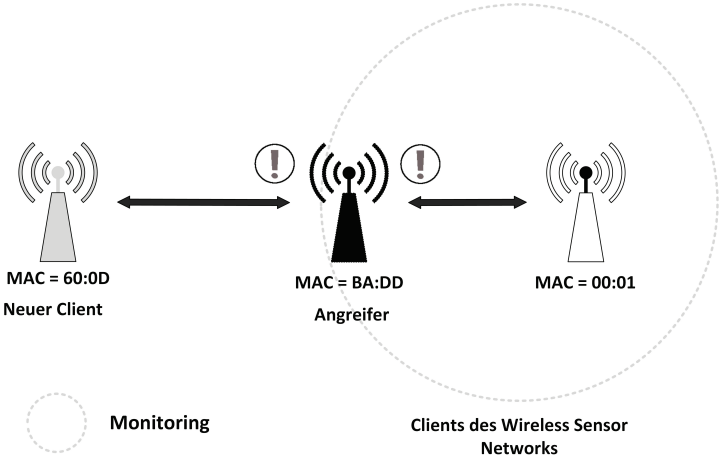

Abb. 6: Monitoring eines Device bei Evil-Twin-Angriff

WSN nach erfolgreichem Pairing. Beide Zustände sind durch unterschiedliche Kommunikationsmuster gekennzeichnet. Agiert ein Device also sowohl als Client bzw. Sensor eines WSN, als auch als Bridge, so sollte dieses Verhalten von anderen Clients erkannt und im Netzwerk weitergegeben werden.

Die Pairing-Phase muss als Modus eines WSN realisiert sein. Dann prüfen alle bestehenden Clients eines WSNs während einer Pairing-Phase alle Netzwerk-Pakete, die sie erhalten, auch wenn sie nicht an diesen Client adressiert sind. Wie in Abbildung 6 dargestellt, werden damit alle Datenströme von unbekannten Clients überwacht. Zur Erkennung von Evil-Twin-Angriffen ist es wichtig, Kommunikation zwischen unbekannten Devices zu überwachen. Ein neuer Client sollte in der Pairing-Phase nur mit dem Device kommunizieren, das den Zugang zum Netzwerk anbietet. Kommunikation mit anderen Devices während dieser Phase ist nicht notwendig und damit potentiell verdächtig.

Wird ein solches Verhalten von Clients im Netzwerk wahrgenommen und die Anzahl übersteigt einen Schwellwert, sollten die Clients diese Beobachtung im Netzwerk weiter geben. Dann kann der Netzwerk-Controller als Reaktion den Pairing-Modus beenden und den bereits an einen potentiellen Angreifer ausgegebenen Schlüssel löschen. Das kann im Rahmen eines *Client Revoke* und einer anschließenden *Key Rotation* zur Sicherung der Integrität geschehen. Dadurch ist es nicht notwendig gesonderte Alarmierungspakete zu senden. Da der Angreifer bei diesem Angriff nicht die bereits durch kryptographische Verfahren gesicherte Verbindung zwischen Client und Netzwerk-Controller stört, sondern unerkannt bleiben möchte, kann diese Verbindung für das Senden der Monitoring-Informationen und Fehlermeldungen benutzt werden.

6.2 Erkennen eines Spoofing-Angriffs

Eine Erkennung des Spoofing ist dadurch nicht möglich, da der Angreifer hier einem neuen Device vorspiegelt ein bestehender Netzwerk-Knoten zu sein. Ziel des Angreifers ist es statt des neuen Devices Bestandteil des Netzwerks zu werden und eine Bridge im Netzwerk zu diesem Device zu bilden. Der vorgeschlagene Ansatz hier ist es, dass das neue Device erkennt, das sich jemand mit der eigenen MAC-Adresse versucht im Netzwerk anzumelden. Dazu können während der Pairing-Phase von dem neuen Device die Adressen von Netzwerk-Paketen analysiert werden, um die Nutzung der eigenen MAC-Adresse durch ein anderes Device zu erkennen.

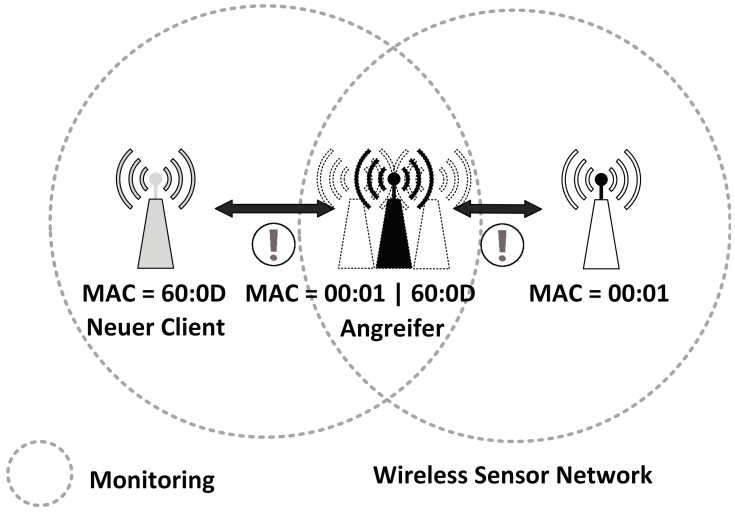

Abb. 7: Erkennung von Spoofing durch Monitoring

Ergänzend wird ein Alarmierungsmechanismus benötigt, um auf den Angriff hinzuweisen, da das neue Device noch nicht Client des WSNs ist.

Als Basis wird dabei der oben dargestellte Ansatz zum Monitoring verwendet. Ein Device kann nicht feststellen, ob zwei aufeinander folgende Netzwerkpakete vom selben Device versendet wurden. Sie müssen sich dabei auf die Angabe der Quelladresse verlassen. Eine Manipulation dieser Quelladresse ist vom Device anhand des Pakets nicht feststellbar. Was man auf der anderen Seite durchaus messen kann, ist den Standort eines Clients in Relation zu Entfernungen zu anderen Netzwerk Clients. Da Clients in WSNs potentiell bewegt werden können, ist die so festgestellte Bewegung eines Clients ein Hinweis, aber kein Beweis für einen Angriff. Weiterhin kann das Device, dessen Adresse vom Angreifer verwendet wurde, Pakete mit seiner eigenen MAC-Adresse als Quelladresse durch Monitoring erkennen (Abbildung 7). Da MAC-Adressen weltweit einheitlich sein sollten, sind ein Fehler oder eine Manipulation eines anderen Devices mögliche Erklärungen für doppelt auftretende Adressen.

Da für diesen Angriff zuerst Selective Jamming durch den Angreifer erfolgt sein muss, um das neue Device vom WSN zu isolieren, besitzt der Angreifer also diese Fähigkeit. Damit kann der Angreifer natürlich auch den Transport von Monitoring-Informationen und Fehlermeldungen in der Payload von Paketen unterbinden. Also muss man zusätzlich Mechanismen für das Senden von Alarm-Nachrichten etablieren, die durch Selective Jamming nicht blockiert werden können. Dazu muss eine Alarm-Nachricht bereits in den Header eines Pakets integriert werden können. Dadurch kann der Angreifer das Senden von Fehlermeldungen und Alarmen mindestens durch Selective Jamming nicht verhindern. Damit können Devices selber duplizierte MAC-Adressen erkennen und das WSN über potentielle Manipulationen informieren.

Das neue Device scannt dazu während der Pairing-Phase plus einem zusätzlichen Intervall alle Netzwerkpakete und prüft, ob die Quelladresse identisch mit der eigenen Adresse ist. In dem Fall gibt es eine duplizierte Adresse im Netzwerk und damit einen potentiellen Spoofing-Angriff. Dann wird eine Fehlermeldung gesendet, sodass alle Clients im Netzwerk informiert werden. Wenn diese Fehlermeldung in Form eines Flags im Header gesendet wird, kann die Meldung nicht durch Selective Jamming blockiert werden, da Selective Jamming erst einsetzt, nachdem der Header verarbeitet wurde.

7 Zusammenfassung

Im Bereich der Wireless Sensor Networks wurden Angriffe in der Pairing-Phase untersucht. Dazu wurden Ansätze zur Erkennung von Angriffen durch Monitoring vorgeschlagen, die auch für Devices mit begrenzten Ressourcen einsetzbar sind.

Aufgrund der aktuellen Bedeutung von WSNs in Anwendungen, wie Smart City, Smart Grid, Smart Home, E-Health und Industrie 4.0 ist eine weitergehende Entwicklung von Ansätzen nötig, um die Robustheit dieser Netzwerke zu optimieren und die Auswirkung von Angriffen zu begrenzen.

Literatur

[ABIS+15] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, C. Wachsmann: SEDA: Scalable Embedded Device Attestation. *In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ACM (2015), 964–975.

[Alli10] Z. Alliance: ZigBee Specification (2010).

[BaGM08] K. Bauer, H. Gonzales, D. McCoy: Mitigating Evil Twin Attacks in 802.11. *In: 2008 IEEE International Performance, Computing and Communications Conference* (2008), 513–516.

[BPCC+07] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, Y. F. Hu: Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. In: *Computer Communications*, 30, 7 (2007), 1655 – 1695.

[DeBa13] S. Devisri, C. Balasubramaniam: Secure routing using trust based mechanism in wireless sensor networks (WSNs). In: *International Journal of Scientific & Engineering Research*, 4, 2 (2013), 1–7.

[DeHM06] J. Deng, R. Han, S. Mishra: INSENS: Intrusion-tolerant routing for wireless sensor networks. In: *Computer Communications*, 29, 2 (2006), 216 – 230, dependable Wireless Sensor Networks.

[Fara08] S. Farahani: ZigBee Wireless Networks and Transceivers. Newnes, Newton, MA, USA (2008).

[FrTA13] A. G. Fragkiadakis, E. Z. Tragos, I. G. Askoxylakis: A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. In: *IEEE Communications Surveys Tutorials*, 15, 1 (2013), 428–445.

[FuRa15] J. D. Fuller, B. W. Ramsey: Rogue Z-Wave controllers: A persistent attack channel. *In: Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th* (2015), 734–741.

[GBMP13] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami: Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. In: *Future Gener. Comput. Syst.*, 29, 7 (2013), 1645–1660.

[HaRa16] J. Hall, B. Ramsey: EZ-Wave. https://github.com/AFITWiSec/EZ-Wave (2016).

[HaZJ06] W. Hang, W. Zanji, G. Jingbo: Performance of DSSS against Repeater Jamming. *In: 2006 13th IEEE International Conference on Electronics, Circuits and Systems* (2006), 858–861.

[HZLH09] L. Huai, X. Zou, Z. Liu, Y. Han: An Energy-Efficient AES-CCM Implementation for IEEE802.15.4 Wireless Sensor Networks. *In: Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on* (2009), Bd. 2, 394–397.

[JiZh07] Y. Jiang, B. Zhao: A secure routing protocol with malicious nodes detecting and diagnosing mechanism for wireless sensor networks. *In: Asia-Pacific Service Computing Conference, The 2nd IEEE*, IEEE (2007), 49–55.

[KaLP03] C. Karlof, Y.-p. Li, J. Polastre: ARRIVE: Algorithm for robust routing in volatile environments. Computer Science Division, University of California (2003).

[LHDH+05] Y. W. Law, L. van Hoesel, J. Doumen, P. Hartel, P. Havinga: Energy-efficient Link-layer Jamming Attacks Against Wireless Sensor Network MAC Protocols. *In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '05, ACM, New York, NY, USA (2005), 76–88.

[LiZL06] P. Li, J. Zhang, Y. ping Lin: Multipath-Based Secure Routing Algorithm for Sensor Network. *In: 2006 6th World Congress on Intelligent Control and Automation* (2006), Bd. 1, 4133–4136.

[LMKG+09] C. Lederer, R. Mader, M. Koschuch, J. Großschädl, A. Szekely, S. Tillich: Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks: Third IFIP WG 11.2 International Workshop, WISTP 2009, Brussels, Belgium, September 1-4, 2009, Proceedings, Springer Berlin Heidelberg, Berlin, Heidelberg, Kap. Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks (2009), 112–127.

[MGKP09] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou: A survey on jamming attacks and countermeasures in WSNs. In: *Communications Surveys & Tutorials, IEEE*, 11, 4 (2009), 42–56.

[OsSM15] R. Ostadal, P. Svenda, V. Matyas: Information Security Theory and Practice: 9th IFIP WG 11.2 International Conference, WISTP 2015, Heraklion, Crete, Greece, August 24-25, 2015. Proceedings, Springer International Publishing, Cham, Kap. On Secrecy Amplification Protocols (2015), 3–19.

[PeSW04] A. Perrig, J. Stankovic, D. Wagner: Security in Wireless Sensor Networks. In: *Commun. ACM*, 47, 6 (2004), 53–57.

[PeZB95] R. L. Peterson, R. E. Ziemer, D. E. Borth: Introduction to spread-spectrum communications, Bd. 995. Prentice Hall New Jersey (1995).

[PLGP06] B. Parno, M. Luk, E. Gaustad, A. Perrig: Secure Sensor Network Routing: A Clean-slate Approach. *In: Proceedings of the 2006 ACM CoNEXT Conference*, CoNEXT '06, ACM, New York, NY, USA (2006), 11:1–11:13.

[ShGh10] K. Sharma, M. Ghose: Wireless sensor networks: An overview on its security threats. In: *IJCA, Special Issue on Mobile Ad-hoc Networks MANETs* (2010), 42–45.

[SKKM15] J. Singh, R. Kumar, V. Kumar, A. Mishra: Intruder detection by visual cryptography in wireless sensor networks. *In: Communications and Signal Processing (ICCSP), 2015 International Conference on* (2015), 1422–1425.

[VHPARS+13] N. Vidgren, K. Haataja, J. L. Patiño-Andres, J. J. Ramírez-Sanchis, P. Toivanen: Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned. *In: System Sciences (HICSS), 2013 46th Hawaii International Conference on* (2013), 5132–5138.

[WMSL11] M. Wilhelm, I. Martinovic, J. B. Schmitt, V. Lenders: Short Paper: Reactive Jamming in Wireless Networks: How Realistic is the Threat? *In: Proceedings of the Fourth ACM Conference on Wireless Network Security*, WiSec '11, ACM, New York, NY, USA (2011), 47–52.

[YaZh08] X. Yao, X. Zheng: A Secure Routing Scheme Based on Multi-Objective Optimization in Wireless Sensor Networks. *In: Computational Intelligence and Security, 2008. CIS '08. International Conference on* (2008), Bd. 1, 436–441.

[ZiSt15] T. Zillner, S. Strobl: ZigBee Exploited - The good, the bad and the ugly. https://www.blackhat.com/us-15/ (2015), black Hat USA.

[ZLCS08] J. Zhou, C. Li, Q. Cao, Y. Shen: An intrusion-tolerant secure routing protocol with key exchange for wireless sensor network. *In: Information and Automation, 2008. ICIA 2008. International Conference on* (2008), 1547–1552.

[ZlGh13] B. Zladi, S. Ghanoun: Security evaluation of the Z-Wave wireless protocol. https://www.blackhat.com/us-13/ (2013), black Hat USA.