Inhaltsverzeichnis

Angreifermodelle für Sensornetze

Sergey Kovalev

26. Januar 2009

Sensornetze sind weit verbreitet. Ursprünglich für Militärzwecke entwickelt, werden Sensornetze heute auch zu Forschungszwecken eingesetzt. Das bedeutet, dass sie zuverlässig sein müssen und eine gewisse Verantwortung zu übernehmen haben. Um diese Kriterien erfüllen zu können, muss man sich in erster Linie Gedanken über die Sicherheit eines solchen Netzes machen. Der beste Weg einen passenden Schutz zu entwickeln ist eine Analyse verschiedener Angriffsmöglichkeiten. Zu diesen Zwecken werden zunächst allgemeine Angriffe modelliert (engl. threat modeling), um später auf konkrete Situationen angewendet zu werden. Dieses Seminar beschäftigt sich mit solchen Modellen. Es wird auf den Aufbau eines Sensornetzes, wie Kommunikation und Protokolle, eingegangen und deren Schwachstellen aus der Sicht eines Angreifers werden betrachtet. Angefangen bei allgemeinen Charakteristiken eines Angreifers, werden Standard-Angriffsmodelle erklärt und deren Anwendung auf konkrete Routingprotokolle gezeigt: TinyOS Beaconing, Directed Diffution, GEAR und GPRS. Wenn man einmal das Prinzip hinter den Angriffen versteht, kann man es benutzen um weitere Angriffsmöglichkeiten zu modellieren. Insgesamt sollte es dazu dienen, die Sicherheit eines Systems zu erhöhen. Das erreicht man dadurch, dass man für jedes Angriffsmodell eine Gegenmaßnahme entwickelt und diese entsprechend umsetzt.

1 Einleitung

Täglich haben wir mit verschiedenen Arten von verteilten Systemen, wie dem Internet, zu tun. Sensornetze gehören auch dazu und auch wenn sie uns weniger auffallen, sind sie häufig im alltäglichen Leben zu finden: z.B. Alarmanlagen und Überwachungssysteme. Diese besitzen bereits gute Sicherheitsprotokolle, die in der Lage sind die meisten Angriffe abzublocken oder gar zu vermeiden. Wenn man selber ein System auf Basis von Sensornetzen entwickelt und auf den Sicherheitsaspekt eingeht, muss man zunächst wissen, wovor man das eigene System zu schützen hat. Man arbeitet mit sogenannten Angreifermodellen. Man geht davon aus, dass ein Angreifer im Besitz bestimmter Eigenschaften und Technologien ist und ein Interesse daran hat, einem Netz einen gewissen Schaden zuzufügen, sei es einfaches Informationsabhören oder Zerstörung des gesamten

Netzes. Seine Absichten, Technologiebesitz und Vorgehensweise können in gewisse Muster unterteilt und in Form eines Modells zusammengefasst werden, welche sich auf konkrete Netzarchitekturen anwenden lassen. Diese Modelle sollen dem Entwickler helfen, sein Netz vor möglichen Angriffen zu schützen, um bei seinem Endprodukt ein sicheres und zuverlässiges System herausbringen zu können.

2 Sensornetze

2.1 Allgemein

Sensornetze[1] sind eine Vernetzung von kleinen, meist billigen, Sensorknoten, welche einen oder mehrere Sensoren haben und in der Lage sind allgemeine Rechenoperationen durchzuführen. Diese Netze bestehen oft aus Hunderten oder Tausendenen einzelner Knoten, die in einem sich selbst organisierendem Ad-hoc-Netz zusammenarbeiten. Dies wird benutzt um eine ausgewählte Umgebung zu überwachen oder diese zu beeinflussen. Ursprünglich setzte man Sensornetze für militärische Zwecke ein, dennoch findet deren Einsatz mittlerweile auch in anderen Gebieten sehr verbreitet statt. So können Sensornetze zur Errichtung einer Alarmanlage oder zur Klimaüberwachung eines Ortes benutzt werden.

Ein Sensornetz kann man normalerweise wie folgt charakterisieren: es hat eine begrenzte Energiekapazität, geringe Speichergröße und Bandbreite, sowie eine kurze Funkreichweite. Diese Charakteristiken führen zu sehr hohen Ansprüchen an das Sicherheitssystem innerhalb eines Sensornetzes, deshalb bietet es sich an eine Public-Key-Kryptographie einzusetzen. Aber aufgrund eines hohen Energiebedarfs ist es weniger sinnvoll diese tatsächlich zu verwenden. Um ein Bit zu verschicken, braucht ein Sensorknoten eine Energiemenge, die äquivalent zum Ausführen von 800-1000 Anweisungen ist. Das heißt, dass jede Erweiterung einer zu versendenden Nachricht, die durch das Einsetzen verschiedener Sicherheitsmechanismen zustande kommt, zu sehr hohen Energiekosten führen kann. Aufgrund der begrenzten Energiekapazität eines Sensorknotens gilt es, dies möglichst zu vermeiden.

2.2 Architektur eines Sensornetzes

Ein Sensornetz hat oft einen oder mehrere Knoten, an welchen sich die zentrale Steuerung befindet. Diese werden als Basisstationen bezeichnet. Eine Basisstation kann dann zum Beispiel an ein weiteres Netz oder an einen hochleistungsfähigen Rechner mit hohen Speicherkapazitäten angeschlossen werden. Man kann diese also als Informationsempfänger charakterisieren. In der Regel hat eine solche Station mehr Energie als jeder andere Knoten im Netz, genug Speicher um alle kryptographische Schlüssel abzuspeichern, einen stärkeren Prozessor und ist zur Kommunikation mit anderen Netzen gedacht.

Die anderen Sensorknoten sind per Funk mit der Basisstation verbunden und werden in einer Routingtabelle gespeichert. Eine Basisstation ist dabei die Wurzel eines Routingbaumes.

2.3 Kommunikationsarchitektur

Die Kommunikation in den Sensornetzen geschieht über einen Funkkanal und kann in folgende Kategorien unterteilt werden:

- Knoten zur Basisstation: wird benutzt um beispielsweise Sensordaten zu versenden
- Basisstation zu einem Knoten, z.B. um die Sicherheitsschlüssel zu erneuern
- Basisstation zu allen Knoten, kann zur Erstellung einer neuen Routingtabelle verwendet werden
- Kommunikation zwischen definierten Gruppen. Diese Verfahren kann zur Reduzierung der gesamten Anzahl von versendeten Nachrichten benutzt werden, um somit z.B. den generellen Stromverbrauch zu reduzieren.

3 Angreifermodelle

3.1 Schwachstellen eines Sensornetzes

Wie bereits beschrieben, gehört es zu den Aufgaben eines Sensornetzes, Daten zu sammeln, diese eventuell zu speichern und weiterzuversenden. Es ist natürlich im Sinne des Netzbetreibers, die Daten und das Netz vor Angriffen zu schützen, jedoch kann man Angriffe nicht ganz ausschließen. Folgende Punkte zeigen, an welchen Stellen ein Angreifer sich einen Zugang zu einem Sensornetz verschaffen kann:

- Ein Funkkanal, über welchen die Kommunikation in einem Sensornetz erfolgt, ist offen für alle. Es reicht schon aus einen Funkempfänger auf die gleiche Frequenz wie die eines Sensornetzes einzustellen, um in der Lage zu sein, sich die Netzwerkaktivitäten anzeigen zu lassen.
- Die Entwicklung verschiedener Protokolle für die Sensornetze geschieht oft öffentlich oder zumindest nicht völlig geheim, sodass ein Angreifer sich die Struktur der Protokolle angucken und dementsprechend die gefundenen Sicherheitslücken für seine Zwecke verwenden kann.
- Da Sensornetze begrenzte Ressourcen haben, kann man starke Sicherheitsprotokolle nicht implementieren, weil die Algorithmen sehr komplex und zu konstenaufwändig sind. Man muss daher berücksichtigen, dass beim Implementieren eines asymmetrisches Sicherheitsprotokolls hohe Anforderungen an Ressourcen eines einzelnen Knotens gestellt werden, was eine negative Auswirkung auf die Leistungsfähigkeit eines Netzes hat. So muss man für das Finden eines optimalen Sicherheitsprotokolls einen Kompromiss zwischen Sicherheit und Leistungsfähigkeit eingehen. Aus diesem Grund tendiert man oft zu einem symmetrischen oder zu einem schwachen asymmetrischen Sicherheitsprotokoll, welches von einem erfahrenen Angreifer umgangen werden kann.

3.2 Das Dolev-Yao-Angreifermodell

Das Dolev-Yao-Modell[2] ist ein klassisches Angreifermodell, das eine weite Akzeptanz in kryptographischen Protokollen gefunden hat. Dieses Modell ist allgemein und lässt sich dementsprechend auch auf Sensornetze übertragen. Es wird von einem beliebigen Netz ausgegangen, sei es eine Vernetzung von Geräten, Sensoren oder von Rechnern, wie z.B. dem Internet. Ein solches Netz hat viele Teilnehmer und eine beliebige Person kann diesem Netz beitreten und seine Tätigkeiten dort ausführen: empfangen von Informationen, die von den anderen Teilnehmern gesendet werden oder beliebige Informationen an die anderen versenden. Dabei braucht dieser Teilnehmer keine Authorisierung. In so einer offenen Umgebung müssen wir davon ausgehen, dass es auch feindselige Teilnehmer gibt, die nicht nur die versendeten Nachrichten passiv abhören, sondern sich auch aktiv in das Netz einmischen. So können Informationen verändert, neu adressiert, dupliziert, gelöscht oder neu hinzugefügt werden, was zu verschiedenen Störungen im Betrieb eines Netzes führen kann. So kann eine Nachricht beispielsweise destruktive Informationen für einen Empfänger enthalten. Solche feindseligen Teilnehmer werden in der Kryptologieliteratur als aktive Angreifer bezeichnet. Es kann einen einzigen oder eine Gruppe von Angreifern geben, die fremd für das Netz sind, jedoch kann auch ein interner Teilnehmer zu einem Angreifer werden. Es wird davon ausgegangen, dass solch ein Angreifer sich sehr gut mit allen möglichen Arten der Manipulation der Kommunikation auskennt und unvorhersehbar handelt. Wenn es sich dabei um eine Gruppe von Angreifern handelt, kann z.B. durch geschicktes Vorgehen auch die Kontrolle über das gesamte Netz gewonnen werden.

Das Dolev-Yao-Modell erwartet genau so einen Angreifer und charakterisiert ihn mit folgenden Eigenschaften:

- er kann jederzeit beliebige Nachrichten abfangen, die netzintern gesendet werden
- er ist ein berechtigter Teilnehmer des Netzes und kann somit eine Verbindung zu beliebigem weiteren Teilnehmer des Netzes herstellen
- er hat die Möglichkeit auch von den anderen Teilnehmern direkt angesprochen zu werden
- seine Nachrichten können an obere Instanzen unter einer falschen Identität gesendet werden

So geht man davon aus, dass jede im Netz gesendete Nachricht bei einem Angreifer ankommt und jede von den anderen Teilnehmern empfangene Nachricht vom dem Angreifer gesendet wurde. Anders gesagt, im Rahmen des Modells hat ein einziger Angreifer die Kontrolle über das gesamte Netz.

3.3 Angreifermodelle für Sensornetze

3.3.1 Allgemeine Differenzierung

Natürlich kann man bereits existierende Angreifermodelle auf Sensornetze übertragen, jedoch muss man diese auf die Spezifikationen eines Sensornetzes anpassen. Eine wichtige

Zweiteilung[3] der Angreifermodelle besteht darin, dass man zwischen einem *mote-class* Angreifer und einem *laptop-class* Angreifer unterscheidet.

Ein *mote-class* Angreifer hat Kontrolle über einen oder mehrere Knoten in einem Sensornetz. Alternativ kann er auch im Besitz von anderen Sensorknoten sein, welche er dann manipulieren und für die Angriffe benutzen kann.

Ein *laptop-class* Angreifer verfügt über bessere Technologien. Wie der Name schon sagt, könnte er über einen Laptop verfügen und mithilfe weiterer angeschlossenen Hardware, wie z.B. einer Senderantenne, komplexere Angriffe durchführen.

Die zweite Unterscheidung macht man zwischen internen und externen Angriffen, so genannten *insider*- und *outsider*- Angriffen. Dabei geht man bei einem *insider*-Angriff davon aus, dass der Angreifer bereits ein legitimer Netzteilnehmer ist, bzw. zu einem geworden ist, und übt aus dieser Position seinen Angriff aus. Ein *outsider*-Angreifer führt seine Angriffe von außen durch.

Da man in einem Sensornetz wenig Ressourcen zur Verfügung hat, werden die Routing-Protokolle innerhalb eines solchen Netzes einfach gehalten, was die Angriffe oft erleichtert. Die meisten Angriffe auf dem Network-Layer lassen sich in folgende Kategorien[3] unterteilen:

- Verfälschung der Routing-Information
- Selektives Weitersenden von Paketen
- Sinkhole Angriffe
- Wormholes
- Sybil Angriffe
- HELLO flood Angriffe

In einem Sensornetzwerk kann aber auch ein Angriff über den Link-Layer erfolgen. Ein dazugehöriges Beispiel ist

- Spoofing von Acks (Bestätigungen)

Diese Angriffe werden im Folgenden weiter erläutert und man wird sehen, dass die Angriffe grob in 2 Klassen unterteilt werden können: direkte Datenmanipulation und Angriffe auf die Routing Topologie.

Um die verschiedenen Angriffsarten anschaulich zu machen, wird in den entsprechenden Abbildungen die in Abbildung 1 dargestellte Legende benutzt.

3.3.2 Verfälschung der Routing-Information

Hier wird ein direkter Angriff auf die zu versendenden Pakete eines Sensornetzes vorgenommen. Man kann z.B. veraltete Pakete oder Duplikate versenden, sowie eigene Pakete, die falsche Informationen enthalten. Diese, scheinbar harmlosen Pakete, können für viele unerwünschte Folgen zuständig sein: ein Angreifer kann Schleifen innerhalb eines Routings erstellen, den Datenverkehr erhöhen, Routen verkleinern oder erweitern, Latenzzeiten erhöhen usw.

Abbildung 1: Legende[3]

3.3.3 Selektives Weitersenden von Paketen

Auch *selective forwarding* genannt. Viele Netze gehen davon aus, dass die Informationen an den Knoten weitergesendet werden. So kann ein Angreifer beispielsweise die empfangenen Pakete löschen und sich wie ein schwarzes Loch verhalten. Das kann aber nicht immer Erfolg haben, denn ein Knoten könnte Informationen bekommen, dass seine Pakete nicht ankommen, was zur Folge hätte, dass er sich eine neue Route sucht. Daher kann man es etwas anders durchführen, indem nur die ausgewählten Pakete weitergesendet werden.

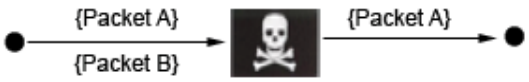

Abbildung 2: Selektives Weitersenden

Diese Angriffe sind sehr effektiv, wenn der Angreifer ein explizierter Teilnehmer des Netzes ist, allerdings kann man diesen Angriff auch als Nicht-Teilnehmer erfolgreich durchführen. Dazu muss man auch in der Lage sein, die versendeten Pakete abhören zu können. Ist das der Fall, kann man für einen Stau innerhalb eines Netzes sorgen oder eine Kollision mit dem ausgewählten Paket verursachen.

3.3.4 Sinkhole Angriffe

In einem Sinkhole Angriff ist das Ziel des Angreifers den gesamten Datenverkehr von benachbarten Knoten an einen einzigen ausgewählten Knoten zu ziehen. Dabei kann dieser Knoten auch der Angreifer selbst sein, was ihm die Möglichkeit gibt, Angriffe anderer Arten durchzuführen. Die Funktionsweise eines Sinkhole Angriffs besteht darin, dass der ausgewählte Knoten für seine Nachbarn und Umgebung besonders attraktiv gemacht

wird. Ein Kriterium für diese Attraktivität kann z.B. das sogenannte „Quality of Service“ sein. Wenn ein Angreifer den benachbarten Knoten einen störungsfreien Kanal mit geringen Latenzzeiten zur Verfügung stellen kann, wird dieser in entsprechenden Protokollen mit höherer Wahrscheinlichkeit zum Versand von Nachrichten benutzt. Des Weiteren gibt es Protokolle, wo ein Knoten, der solch einen Kanal benutzt, ihn an seine Nachbarn propagiert. Das führt zum Ziel des Sinkhole Angriffs und kann jetzt dazu benutzt werden, um weitere Angriffe an dem Netz auszuüben. Da bietet sich z.B. selektives Weitersenden an, da man den Versandkanal bereits unter seiner Kontrolle hat.

3.3.5 Sybil Angriffe

Bei einem Sybil-Angriff täuscht ein einziger Angreifer gleichzeitig mehrere Identitäten vor. Das führt dann dazu, dass in einem Netz mehrere Knoten unter Kontrolle des Angreifers sind und die legitimen Teilnehmer des Netzes ein und denselben Angreiferknoten als mehrere Knoten identifizieren. Folglich kann das zu Verfälschung von Routinginformationen und zu fatalen Folgen in den Netzen führen, wo die Koordinaten einzelner Knoten von Bedeutung sind.

3.3.6 Wormholes

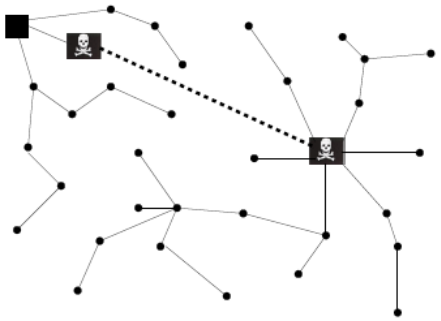

Abbildung 3: Ein Wormhole Angriff auf TinyOS beaconing[3]

Bei einem Wormhole-Angriff greift der Angreifer die Nachrichten von einem Knoten ab und sendet diese in einen anderen Teil des Netzes weiter. Die einfache Art dieses Angriffs kann man schon erreichen, indem man sich zwischen zwei benachbarten Knoten platziert und die Nachrichten zwischen diesen abgreift und weitersendet. Normalerweise wird dies ein wenig anders durchgeführt. Man platziert zwei Angreiferknoten in verschiedenen Teilen eines Netzes. Diese stellen dann einen schnellen Kanal zum Datenaustausch zwischen den jeweiligen Teilen des Netzes zur Verfügung. So kriegen die Nachbarknoten des Angreifers die Information, dass sie weit liegende Knoten über diesen erreichen können. Das wird zur Folge haben, dass ein Knoten denkt, er sei von einem anderen Knoten zwei, drei Hops entfernt, während in Wirklichkeit die Entfernung beispielsweise zehn oder mehr Hops sein könnte. Wie man es vielleicht schon erahnen kann, werden viele

Informationen über den kürzesten Weg verschickt, was automatisch dazu führt, dass die meisten Nachrichten über den Angreiferkanal übertragen werden. Damit hat man einen Sinkhole-Angriff erreicht.

Die durch den Angriff erreichte Struktur kann man sehr gut für das Abhören oder selektives Weiterleiten der Nachrichten benutzen. Wenn dabei der Angreifer, wie bei einem Sybil-Angriff, mehrere Identitäten vortäuscht, kann es recht schwer werden diesen Angriff überhaupt festzustellen.

3.3.7 HELLO flood Angriffe

Viele Protokolle basieren darauf, dass die Teilnehmerknoten HELLO-Pakete versenden müssen. Wenn diese Pakete von den Nachbarn empfangen werden, registrieren diese den Absender auch als deren Nachbar. Wenn ein Knoten ein solches Packet empfängt, kann er auch annehmen, dass er sich in der normalen Sendeweite vom Sender befindet. Diese Annahme, kann aber auch fälschlich sein: wenn ein Angreifer eine starke Senderantenne hat, kann er die HELLO-Pakete an alle Teilnehmer des Netzes senden, sodass jeder dieser Knoten sich denkt, der Angreifer sei sein direkter Nachbar.

Ein Beispiel dazu: ein Angreifer sendet HELLO-Pakete an alle Netzteilnehmer über eine Leitung einer hohen Qualität. Die somit angegriffenen Knoten registrieren den Angreifer als deren Nachbarn und werden versuchen diese gute Leitung zum Versenden von Informationen zu benutzen. Da der Angreifer aber oft viel zu weit von diesen Knoten entfernt ist, werden die Pakete ins Leere verschickt, was natürlich eine globale Störung im Routingsystem hervorruft. Wenn ein Knoten merkt, dass seine Verbindung zum Angreifer gar nicht existiert, versucht er seine Informationen mittels seiner Nachbarn zu versenden, welche sich wiederum in der gleichen Situation befinden und auch an den Angreifer senden wollen.

Um einen HELLO-Flood Angriff durchführen zu können, muss man nicht unbedingt in der Lage sein eine eigene HELLO-Nachricht zusammenzustellen. Es reicht schon ein HELLO-Packet abzugreifen und diesen über eine gute Leitung an alle weiteren Knoten zu versenden.

3.3.8 Spoofing von Acks

Auch auf dem Link-Layer können in einem Sensornetz Angriffe erfolgen. Das hängt damit zusammen, dass manche Routingprotokolle für die Sensornetze teilweise implizit aber auch explizit auf den Bestätigungsnachrichten (Acknowledgements = Acks) basieren. Dafür werden zunächst Pakete abgefangen und abgehört. Danach erfolgt die Versendung eines Acks an den Sender. Das Ziel bei diesem Angriff besteht darin, dem Sender eine schlechte als eine starke Leitung oder einen inaktiven, „toten“ Knoten als aktiv vorzutäuschen. Da die über eine schwache oder nicht existierende Leitung versendeten Pakete in Wirklichkeit verloren gehen, hat der Angreifer die Möglichkeit die Pakete selektiv weiterzuleiten oder diese für seine Zwecke zu benutzen.

3.4 Angriffe auf Sensornetzspezifische Protokolle

Alle Netzwerkprotokolle, die in den Sensornetzen benutzt werden, sind oft leicht angreifbar. Es könnte sogar passieren, dass durch das Versenden eines einzigen Pakets das komplette Netzsystem zum Zusammenbruch kommt. Die folgenden Unterpunkte beschäftigen sich mit oft benutzten Protokollen, die in Sensornetzen eingesetzt werden und beschreiben deren Schwächen, die zum Angriff benutzt werden können.

3.4.1 Tiny OS beaconing

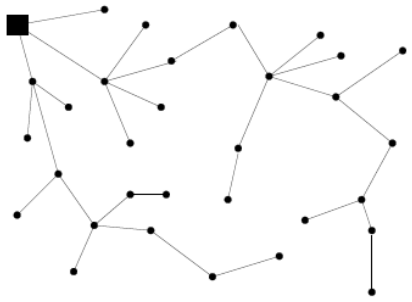

Abbildung 4: Tiny OS beaconing Baum mit einer Basisstation [3]

Beschreibung: Tiny OS beaconing Protokoll[4] basiert darauf, dass unter den teilnehmenden Sensorknoten ein Baum aufgespannt wird (Abb. 4), mit einer Basisstation in der Wurzel dieses Baumes. In bestimmten Zeitabständen sendet die Basisstation ein Routing-Update. Die naheliegenden Teilnehmerknoten markieren den Sender als deren Elternknoten. Danach werden die Pakete weitergesendet, solange bis die letzten Teilnehmer erreicht werden. Am Ende dieser Operation liegt ein Routing-Baum vor, der weiterhin für die Übertragungen im Netz benutzt wird. Um ein Paket zu versenden, wird dieser nun rekursiv an den Elterknoten weitergeleitet bis die Basisstation erreicht ist.

Angriffe: Es lässt sich bereits erahnen, dass das Protokoll selbst sehr anfällig gegen Angriffe. Da die Routingupdates nicht authentifiziert sind, kann jeder Teilnehmerknoten zu einer Basisstation werden und somit den gesamten Traffic innerhalb des Netzes an sich ziehen. Wenn man die Routingupdates authentifiziert machen würde, wäre es dennoch für einen Laptop-class Angreifer möglich zu einer Basisstation zu werden. Dies ermöglicht einen kombinierten Wormhole-/Sinkhole-Angriff durchzuführen.

Wenn ein Angreifer einen ausreichend starken Transmitter hat, kann man einen Angriff mithilfe von HELLO-Paketen durchführen. Zu diesem Zweck wird zunächst ein HELLO-Flood Angriff durchgeführt, welcher eín Routing Update verursacht, wobei jeder Knoten den Angreifer als seinen Elternknoten markiert. Bei entsprechender Reichweite des Signals, das vom Angreifer kommt, wird dieses zur Folge haben, dass die meisten Knoten in dem angegriffenen Netz deren Informationen ins Nirgendwo bzw. an den Angreifer schicken. Somit hat man einen Sinkhole Angriff an dem Netz ausgeführt (Abb. 5).

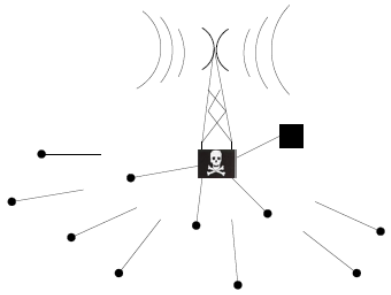

Abbildung 5: HELLO Flood Angriff auf Tiny OS[3]

Weiterhin ist es auch möglich eine Schleife im Routing zu erstellen. Dafür sucht sich der Angreifer zwei Knoten aus (A und B), die in der Funkreichweite des anderen liegen. Danach erfolgt ein Routing Update, welches von dem Angreifer ausgeht: Knoten B kriegt dieses Update, wo Knoten A als Sender spezifiziert ist. Knoten B denkt nur, dass A sein Elternknoten sei und sendet ebenfalls ein Routingupdate an den Knoten A. Da Knoten A bisher noch keine Updates bekommen hat und dieses nun vom Knoten B kommt, wird der letzte ebenfalls als Elternknoten markiert. Wenn nun beliebige Informationen an einen der beiden Knoten ankommen, werden die Pakete zwischen A und B hin- und hergeschickt.

3.4.2 Directed Diffusion

Beschreibung: Bei Directed Diffusion[5] handelt es sich um ein Netzwerkprotokoll, bei welchem zur Lösung der gestellten Aufgabe kein konkreter Knoten angesprochen wird. Es ist die Aufgabe eines Knoten anhand der Anfrage (Interest) zu erkennen, ob er die Aufgabe erfüllen kann oder nicht. Directed Diffusion lässt sich in 3 Phasen einteilen. Zunächst wird vom einem beliebigen Knoten eine Anfrage (Interest) propagiert (Flooding). Dieser wird als Senke bezeichnet. Mit der Verbreitung des Interests wird die Richtung des Datenflusses in Form sogenannter Gradienten (Abb. 6(a)) markiert. In der zweiten Phase senden die Knoten, die die gestellte Anfrage erfüllen können, ihre Informationen über verschiedene Wege zurück zur Senke. In der dritten Phase wählt die Senke für sich die optimalen Wege zum weiteren Informationsversand. Dies wird als Reinforcement (Abb. 6(b)) eines Wegs bezeichnet.

Angriffe: Da die Anfrage mittels Flooding erfolgt, ist es schwierig die Interests vom sicheren Ankommen abzuhalten. Doch sobald ein Knoten seine Informationen über das Netz zu senden anfängt, könnte man die Angriffe in folgende Kategorien unterteilen.
Suppression: Als Ziel wird gesetzt die gesendeten Informatinspakete nicht bei dem Knoten, der das Interest gestellt hat, ankommen zu lassen. Dies kann durch Spoofing von negativen Reinforcements gemacht werden, sodass jeder Weg von der Quelle bis zur Senke verhindert wird.
Duplizieren: ein einfaches duplizieren von Interests kann zum Abhorchen von Informa-

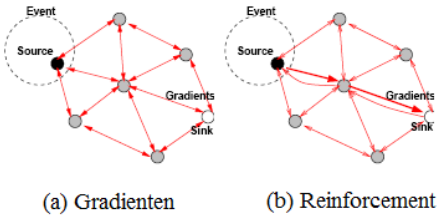

Abbildung 6: Gradienten und Reinforcements bei Directed Diffusion[5]

tionen benutzt werden. Dabei reicht es dem Angreifer ein Interest abzufangen und dieses erneut im Netz zu verbreiten. Da der Angreifer nun der Absender ist, werden die seinem Interesse entsprechenden Informationen zu ihm fließen.

3.4.3 Geographic Routing

Beschreibung: Um die Angriffe auf Geograpic Routing anschaulich zu machen, werden folgende zwei Protokolle betrachtet: GRPS [6] und GEAR [7]. Bei beiden Protokollen werden Daten nicht an einzelne Empfänger gesendet, sondern an bestimmte Koordinaten. Pakete werden zunächst an die sich in der Funkreichweite befindenden Knoten weitergesendet, die einen kleineren Abstand zum Ziel aufweisen. Ein Datenpaket wird genau dann einem Knoten zugewiesen, wenn dieser den geringsten Abstand von den Zielkoordinaten besitzt. Beim GEAR Protokoll wird zusätzlich noch darauf geachtet, wie der Energiestand eines einzelnen Knotens ist.

Angriffe: ein naheliegendes Modell eines Angriffs ist die Vortäuschung einer beliebigen Koordinate. Wenn es sich um GEAR Protokoll handelt, wird der Angreifer auch den Energiestand als maximal angeben. So kann ein Angreifer sowohl den Datenverkehr in seiner Umgebung über sich laufen lassen, als auch der Zielempfänger sein.
Weiterhin kann ein Angreifer einen Sybil-Angriff durchführen, indem er seine Identität mehrfach vortäuscht. Dies kann anhand eines Beispiels [3] gut erklärt werden. Der An-

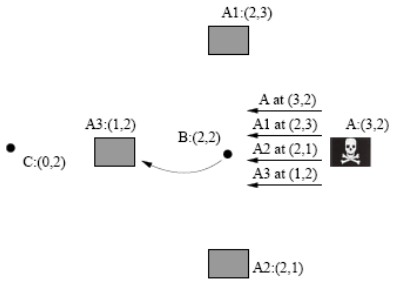

Abbildung 7: Sybil Angriff auf ein GEAR-Netz [3]

greifer A, der auf der Position (3,2) positioniert ist, täuscht seine und 3 weitere nicht existierende Koordinaten vor. Wenn ein Knoten B ein Paket zu der Koordinate (2,0) senden will und bereits die Updates von dem Angreifer erhalten hat, wird er versuchen dies über den Knoten A3:(1,2) zu machen, da dieser in seiner Reichweite und näher als alle anderen am Ziel liegt. Zusätzlich kann natürlich vorgetäuscht werden, dass all die Knoten einen maximalen Energiestand haben, um eventuelle weitere existierende Nachbarn von der Übertragung auszuschließen. Also wird die Übertragung über den Angreifer geschehen und der Datenfluss kann abgefangen und modifiziert werden, was eine gute Voraussetzung z.B. zum selektiven Weitersenden ist.

Ein gutes Beispiel für einen Angriff auf GPRS ist das Erstellen einer ewigen Schleife. Man nehme an, dass das Netz eine wie im Bild 8 abgebildete Topologie hat und die Funkreichweite sich auf einen einzigen Nachbarn beschränkt. Jetzt will der Knoten B(0,1) einen Paket zur Position (3,1) versenden und der Angreifer täuscht dem Knoten C eine falsche Position von B mit (2,1) vor. C kriegt diesen Paket und versucht es an B zu versenden, weil laut seiner Information die Zielkoordinate dem Knoten B nahe liegt. Der echte Knoten B(0,1) kriegt den Paket wieder, da sonst keine weiteren Knoten in der Reichweite sind, und versendet es wieder an C.

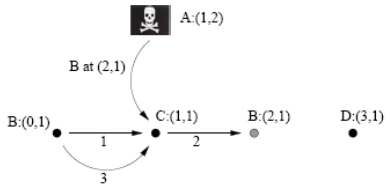

Abbildung 8: Erstellen einer ewigen Schleife bei GRPS [3]

4 Zusammenfassung

Wie man sieht, hat jedes System seine Schwächen. Das größte Problem für die Sicherheit eines Sensornetzes ist wohl die Hardware, die zur Realisierung komplexer Sicherheitsalgorithmen zu geringe Energiekapazitäten hat. Die Software muss dementsprechend angepasst werden. Kenntnisse über das Zielsystem und Verständnis über dessen Funktionsweise können bereits einfache Angriffe ermöglichen. Es gibt viele Standardangriffsarten, die mit einer hohen Wahrscheinlichkeit im Falle eines Angriffs benutzt werden. Dieses Wissen ermöglicht es, die Sicherheit eines Zielsystems zu erhöhen. Threat Modeling ist bereits zu einem wichtigen Bestandteil des Softwareentwicklungsprozesses geworden und darf auch bei Protokollen in Sensornetzen nicht außer Acht gelassen werden. Weiterentwicklungen, die mithilfe von Angriffsmodellen gemacht werden, sollen für mehr Sicherheit sorgen. Es ist besser, bereits am Anfang in Sicherheit zu investieren, bevor die durch einen Angriff verursachten Schäden die Kosten explodieren lassen.

Literatur

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38:393–422, 2002.

[2] Wenbo Mao and Wenbo Mao. A structured operational modelling of the dolev-yao threat model.

[3] D. Karlof, C. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop*, 11 May 2003.

[4] Li Hui Li Anqi Sun Zheng, Zhang Xiao-guang. The application of tinyos beaconing wsn routing protocol in mine safety monitoring. In *Mechtronic and Embedded Systems and Applications, 2008. MESA 2008*, 2008.

[5] Deborah Estrin Chalermek Intanagonwiwat, Ramesh Govindan. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000.

[6] Brad Karp and H. T. Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. pages 243–254, 2000.

[7] D. Estrin Y. Yu, R. Govindan. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. In *Tech. Rep. UCLA/CSD-TR-01-0023*, 2001.